Note: This document is a tentative translation of "Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies" for purpose of reference and its accuracy is not guaranteed. Any entity does not accept responsibility for any disadvantage derived from the information described in the document.

Common Standards for Cybersecurity Measures for Government Agencies and Related Agencies (FY2023)

July 4, 2023

Established by the Cybersecurity Strategic Headquarters

Table of contents

Chapter 1 General Provisions

1.1 Purpose and Scope of these Common Standards for Measures

(1) Purpose of these Standards

The basic principle of information security is to ensure "confidentiality", "integrity", and "availability" of the information handled by government agencies, incorporated administrative agencies, and designated corporations (hereinafter referred to as "Agencies") according to the degree of importance of information, and it is a fundamental responsibility for each government agency to duly implement measures to ensure information security. However, under the current circumstances where the Agencies use and share the common IT environment as well as information, it is necessary to formulate a unified framework to raise the level of information security standards across the agencies.

These Common Standards constitute information security measures deemed necessary in a shared manner across all of the Agencies. Their purpose is to strive to uniformly raise the level of information security of Agencies by regulating matters that the Agencies must comply with for each information security measure (hereinafter referred to as "requirements") as necessary conditions for implementing the Common Model within the common framework for Agencies in accordance with the Common Model of Cybersecurity Measures for Agencies (established by the Cybersecurity Strategic Headquarters).

(2) Scope of these Standards

(a) These Standards shall apply to all employees engaged in administrative services at Agencies.

(b) These Standards shall apply to the information defined below:

(i) Information recorded on the systems for providing information processing or communication, or on external electromagnetic recording media procured or developed by the Agencies to be used by employees to perform their duties (including information described on a paper outputted from the said system or information described on a paper inputted into the said system).

(ii) Information for use of employees, recorded on other information systems or other external storage media (including the information printed out from, or input in the system).

(iii) In addition to (i) and (ii), information concerning the design or operational management of the system procured or developed by Agencies.

(c) These Standards shall apply to all information systems which process the information stipulated herein.

(3) Revisions of these Standards

It is important to precisely understand changes in circumstances and accordingly review information security measures to maintain an appropriate level of information security. Therefore, these Standards shall be regularly reviewed and necessary additions and amendments shall be

made according to information technology development. These Common Standards are drafted by the National center of Incident readiness and Strategy for Cybersecurity (NISC) and finalized by the Cybersecurity Strategic Headquarters via the Cybersecurity Measures Promotion Committee (decided on February 10, 2015 by Chair of the Cybersecurity Strategic Headquarters). Based on regular inspection results on new threats and the operations of Agencies, NISC formulates a draft with the following point(s) in mind:

(a) The Common Standards shall cover the information security measures commonly necessary to all Agencies and shall be formulated with consideration given to conformity with international standards, etc. as well as reflect the current state so as to allow for the Agencies to comply with the specified system of responsibility, implementation framework, and specific measures.

(4) Compliance with laws and regulations

When taking information security measures, laws and regulations which stipulate handling of information and information systems (hereinafter referred to as "relevant laws and regulations") should be respected in addition to these standards. These Standards provide no reference to such relevant laws and regulations, as they should be respected regardless of information security measures. Equally the government's resolutions set forth in response to changing environment of information security should be duly observed.

(5) Government agency's own standards

In these Common Standards, measures to be implemented by Agencies are classified into three layers, namely chapters, sections, and items according to the purpose, with the purposes, general intent, and requirements specified for each item.

The Guidelines for Establishing Agencies' Standards for Information Security Measures formulated separately by the NISC enumerate basic measures that must be taken in order to meet the requirements of the Common Standards (hereinafter referred to as "basic measures"), while also offering explanations of the approaches for formulating and implementing standards. Since the basic measures comply with the requirements, Agencies must meet the corresponding requirements by taking the measures enumerated in the basic measures or measures that are equal to or greater than these.

In addition, Agencies must set in place operational rules and implementation procedures to implement measures prescribed in the standards they formulated.

1.2 Classification of Information and Handling Restrictions

(1) Classification of information

These Standards classify information in three aspects namely confidentiality, integrity, and availability, whose definition are shown below.

When changing or adding the definitions of classifications at Agencies, each Agency must handle information categorized according to the definitions below via a level of security established in

the requirements of these Common Standards or an equal or greater level of security. When providing information to other Agencies, Agencies must ensure that they appropriately communicate regarding the classifications set forth in their own standards, as well as responses for the classifications in these Common Standards.

Classifications for confidentiality

Classification	Classification criteria
Confidentiality class-3 information	Among information handled as part of the work of national administrative organs, information required to be handled as confidential documents prescribed in the Guidelines for Management of Administrative Documents (decided by the Prime Minister, on April 1, 2011; hereinafter referred to as "Document Management Guidelines") Among information handled as part of the work of Incorporated Administrative Agencies and Designated Corporations, information corresponding to the above
Confidentiality class-2 information	Among information handled as part of the work of national administrative organs, except for Confidentiality class-3 information, items which include information with high probability of being regarded as Non-Disclosure Information stipulated in Article 5 of the Act on Access to Information Held by Administrative Organs (Act No. 42 of 1999; hereinafter referred to as "Information Disclosure Act"). Among information handled as part of the work of Incorporated Administrative Agencies, except for confidentiality class-3 information, items which include information with high probability of being regarded as Non-Disclosure Information in each item of Article 5 of the Act on the Protection of Personal Information Held by Incorporated Administrative Agencies, etc. (Act No. 140 of 2001; hereinafter referred to as the “Incorporated Administrative Agencies, etc. Information Disclosure Act”). Moreover, the same shall apply to those Designated Corporations that are listed in Appendix I of the Incorporated Administrative Agencies, etc. Information Disclosure Act (hereinafter referred to as “Designated Corporations listed in the appendix”). Among information handled as part of the work of Designated Corporations other than Designated Corporations listed in the appendix, information corresponding to the above.
Confidentiality class-1 information	Among information handled as part of the work of national administrative organs, information which does not include items which should be regarded as Non-Disclosure Information stipulated in each paragraph of Article 5 of the Information Disclosure Act. Among information handled as part of the work of Incorporated Administrative Agencies or Designated Corporations listed in

	the appendix, information which does not include items which should be regarded as Non-Disclosure Information stipulated in each paragraph of Article 5 of the Information Disclosure Act. Among information handled as part of the work of Designated Corporations other than Designated Corporations listed in the appendix, information corresponding to the above.

Information which comes under Confidentiality class-2 information and Confidentiality class-3 information is called “confidential information”.

Classifications for integrity

Classification	Classification criteria
Integrity class-2 information	Among information for administrative use (except for written information), items whose manipulation, errors, and damage may infringe citizens' rights or hamper proper administrative operations (except for negligible cases).
Integrity class-1 information	Information other than Integrity class-2 information (except for written information)

Note that Integrity class-2 is called “critical information”.

Classifications for availability

Classification	Classification criteria
Availability class-2 information	Among information for administrative use (except for written information), items whose disappearance, loss, or unavailability may infringe citizens' rights or stable administrative operations (except for negligible cases).
Availability class-1 information	Information other than Integrity class-2 information (except written information.)

Note that Availability class-2 information is called “vital information”.
Also, information classified as any of confidential information, critical information, or vital information is called “classified information”.

(2) Types of handling restrictions

"Handling restrictions" means restrictions to ensure proper handling of information by employees, such as to prohibit copying, removing, and distributing information, as well as mandatory encryption and disposal of the data after use.

The employees should appropriately handle the information according to its classification, and follow the types of handling restrictions to demonstrate proper and practical handling of the information. Agencies should set forth the basic definitions of handling restrictions from perspectives of three aspects, namely confidentiality, integrity, and availability.

1.3 Definition of Terms

【A】

- "Applications and contents" means a collective term for application programs, web contents and so forth developed and provided by Agencies.
- "Areas requiring control measures" means areas under the control of the Agencies (including facilities leased by said Agency from external Agencies), where control measures for the facilities and work environment are required to protect information handled.
- "Agencies" means government agencies, incorporated administrative agencies, and designated corporations.

【C】

- "Cloud services" means a capabilities which is offered via a paradigm for enabling network access to scalable and elastic pool of shareable physical or virtual resource with self-service provisioning and administration on-demand, by the provider-defined interface, and is flexible about setting of information security condition adequately. Examples of cloud services include SaaS (Software as a Service), PaaS (Platform as a Service), and IaaS (Infrastructure as a Service). Cloud services as mentioned in these Common Standards specifically refer to cloud services where a non-Agency provides some or all of the functions of an information system to the general public, handling Agencies' information on such services.
- "Cloud service administrator" means an employee of Agencies engaging in the management of a cloud service as designated by the person authorized to permit use applications when approval is given for the use of the cloud service.
- "Cloud service provider" means an operator providing a cloud service.
- "Cloud service users" means employees of Agencies who use a cloud service, or in cases of subcontracting, employees of a subcontractor when the cloud service is used by the subcontractor.
- "Communication line" means mechanisms for transmitting and receiving information among several information systems, and also among several equipment (including devices not purchased by Agencies), as well as between information systems and equipment, using prescribed communication protocol. Unless otherwise specified, it is a generic term referring to the communication lines used for information systems at Agencies. Communication line

includes the one which is not directly managed by Agencies and also includes all connections regardless of their types (such as wire or wireless, physical or virtual).

- "Communication line equipment" means a device which connects communication lines, as well as communication lines and information systems, and controls information transmitted and received over these lines. Communication line equipment includes hubs, switches, routers, and firewalls. Communication line equipment that has physical hardware is referred to as "physical communication line equipment."
- "Communication line inside the Agencies" means a communication line used for communication between the server equipment and terminals managed by an Agency or a shared government system administrator agency, which has no logical connection with the server equipment and terminals not being managed by said Agency. Communication lines inside the Agency also include those physical lines that are not managed by the Agency, such as proprietary lines and VPNs.
- "Communication line outside the Agency" means a communication line other than "Communication line inside the Agency".
- "Subcontracting" means subcontracting part or all of tasks of an Agency, including all forms of agreement such as "mandate," "quasi-mandate," or "contract"; however, only when the Agency's information is handled in those tasks.
- "CSIRT" means a system established at Agencies to respond to information security incidents which occur therein. An acronym for Computer Security Incident Response Team.
- "CYMAT" means a system established in the National center of Incident readiness and Strategy for Cybersecurity which provides proactive support for information security incidents which require unified actions with the government, in the event of, or fear of information security failure at Agencies due to cyber-attacks and so forth. An acronym for Cyber Incident Mobile Assistance Team (information security emergency support team).

【E】

- "Employees" means legal employees such as government officials engaged in administrative work at national administrative organs, executives of Incorporated Administrative Agencies and Designated Corporations engaged in the work of said Agencies, and other people serving under the supervision of other Agencies who handle information and information systems managed by the Agencies. Employees also include dispatched workers and trainees accepted temporarily, though it depends on individual work conditions.
- "Equipment, etc." means a collective term for information systems components (such as servers, terminals, communication line equipment, multiple function devices and other apparatus for specified purposes, and software), as well as external storage media.
- "Equipment for specific purposes" means information system components for specific purposes as in the systems for TV conference, IP phones, network cameras, entry control systems, facility management systems, environment monitoring systems, and so forth, which are equipped with

either a function that connects to a communication line or built-in electromagnetic recording media.

【G】

- "Government agency's own standards" means standards for information security measures to ensure information security of information and systems at Agencies.
- "Government domain name" means a domain name ending with ".go.jp." Government agencies, Incorporated Administrative Agencies, and special corporations (except for special companies) may register (acquire) this domain name.
- "GSOC" means a system established in the National Center of Incident Readiness and Strategy for Cybersecurity to collect information across government, analyze attacks, provide advice to government agencies, and promote collaborations and information sharing among relevant government agencies, 24 hours a day, every day. An acronym for Government Security Operation Coordination Team. GSOC consists of GSOC 1, which covers government agencies, and GSOC 2, which covers incorporated administrative agencies and designated corporations.

【H】

- "Headquarters audit" means an audit conducted by the Cybersecurity Strategic Headquarters pursuant to Article 26 Paragraph (1) Item 2 of the Basic Act on Cybersecurity.

【I】

- "Implementation procedures" means practical procedures need to be determined beforehand to implement the measures prescribed in the standards for measures for individual information systems and tasks of Agencies.
- "Information" means the information set forth in "1.1. (2) Scope of these standards" (b) of the Common Standards.
- "Information security rules" is a collective term for all standards for measures, operational rules, and operating procedures implemented by Agencies.
- "Information security incidents" means information security incidents set forth in JIS Q 27000:2019.
- "Information security measure promotion structures" mean structures established within the Agencies in order to perform duties related to promoting the information security measures of the Agencies in question.
- "Information system" means systems consist of hardware and software (including those managed by outsourcing subcontractors and shared government systems), which are used for information processing or communications, and developed and procured by Agencies unless otherwise specified.

【L】

- “Labeling, etc.” means a measure to make information's classification clear to all who handle the information. This means to display the classification of information and any other actions to make the information classification a common knowledge. One of the examples of such measure is, to indicate the classifications of information recorded in a specific information system by describing them in regulations, and to make them known to all the users of said system.

【M】

- “Measures promotion plan” means a plan to organizationally and continuously implement, and comprehensively promote, information security measures.

【N】

- “National administrative organs” collectively refers to organizations stipulated by law and established within or under jurisdiction of the Cabinet, the Imperial Household Agency, organizations stipulated in Article 49 Paragraph (1) or (2) of the Act for Establishment of the Cabinet Office (Act No. 89 of 1999), organizations stipulated in Article 3 Paragraph (2) of the National Government Organization Act (Act No. 120 of 1948), or other organizations which fall under these organizations.

【O】

- “Operational rules” means the specific rules and standards that need to be established in advance in order to apply the measures set forth in the Government agency’s own standards to the individual information systems and operations.

【S】

- “Server equipment” means the components of information system which provide own services to terminals and other devices getting access to it via communication lines and other means (including components such as pre-loaded software, built-in mouse and keyboard), and unless otherwise specified those procured or developed by Agencies (including those provided by a shared government system). Furthermore, server equipment that has physical hardware is referred to as “physical server equipment.”
- “Shared government system” means an information system that is managed or operated by an Agency for the purpose of shared use among other Agencies and falls under any of the following: a) the information system that coordinates with information systems maintained by other Agencies to provide information security functions; b) the information system used by employees of other Agencies through the equipments provided by the information system. Agencies that develop and operate a shared government system are specifically referred to as “shared government system administrator agencies,” and Agencies that develop and operate an information system using the security function provided by a shared government system and

Agencies that use the equipment, etc. provided by a shared government system are specifically referred to as “shared government system user agencies.”

【T】

- “Terminal” means the equipment of information system component, which employees directly operate to perform information processing (including installed software and peripheral devices such as keyboard and mouse directly connected and treated as an integral part of the equipment), and unless otherwise specified those procured or developed by the Agencies (including those provided by a shared government system). “Terminal” also means mobile terminals. In particular, otherwise specified case examples would include “non-Agency-furnished terminals”, which indicate terminals that were neither procured nor developed by the Agency. In addition, both terminals procured or developed by Agencies and non-Agency-furnished terminals are collectively referred to as “terminals (including non-provided terminals).” Terminals that have physical hardware are referred to as “physical terminals.”

Chapter 2 Basic Framework of Information Security Measures

2.1 Introduction and Plan

2.1.1 Establishment of organizations and systems

Purpose

Implementation of information security measures can be accomplished when employees therein fully understand the authority and responsibilities related to their job positions and functions, and duly fulfil those responsibilities. To achieve this it is essential to clearly define such authority and responsibilities and establish necessary organizations and systems. In particular, the chief information security officer should direct and encourage the entire Agency to systematically execute measures to ensure a steady promotion of information security measures.

The chief information security officer can delegate part of their own responsibilities stipulated in these Common Standards to responsible officers in charge set forth in these Common Standards, such as their deputy chief information security officer.

Compliance Requirements

(1) Designation of the chief information security officer and deputy chief information security officer

(a) The chief information security officer shall be designated to direct tasks associated with information security measures at Agencies.

(b) Agencies may, as needed, designate one deputy chief information security officer who assists the chief information security officer by organizing work related to information security at the Agency and oversee work related to the Agency's information security under the orders of the chief information security officer.

(2) Establishment of the Information Security Committee

(a) The chief information security officer shall establish the Information Security Committee, which consists of representatives of the information security measure promotion structure and of departments engaged in other operations, and whose function is to deliberate over provisions such as standards.

(3) Designation of the chief information security auditor

(a) The chief information security officer shall designate the head information security auditor who directs tasks associated with audits conducted under the direction of the chief information security officer.

(4) Designation of the head information security officer and information security officers

(a) The chief information security officer shall designate an information security officer who directs tasks of information security measures for each unit of organization where the same quality of such measures can be implemented due to the characteristics of their duties. One of the information security officers shall be designated by the chief information security

officer as the head information security officer, who directs all information security officers and assists the chief information security officer and deputy chief information security officer.

(b) Information security officers shall designate an area information security officer who directs tasks of information security measures for each area set forth in the compliance requirements 3.2.1(2)(a).

(c) Information security officers shall designate a division/office information security officer for each office who directs information security related work.

(d) In the planning phase of such information security, information security officers shall designate information system security officers who are responsible for tasks concerning information security measures in the divisions under their management.

(5) Designation of the chief information security advisor

(a) The chief information security officer shall designate the chief information security advisor with expertise and experience in information security, and define the job descriptions of the position including advisory functions for the chief information security officer.

(6) Establishment of an information security measure promotion structure

(a) The chief information security officer shall establish an information security measure promotion structure and stipulate its duties.

(b) The chief information security officer shall designate the person in charge of the information security measure promotion structure.

(7) Establishment of the system for information security incidents

(a) The chief information security officer shall manage and clarify the role of CSIRT.

(b) The chief information security officer shall designate employees deemed to have expertise and competence in information security as officers in charge of CSIRT. One of the CSIRT officers shall be designated as the head CSIRT officer who directs measures in the event of information security incident at Agencies. The chief information security officer shall designate the employees in charge of management inside of CSIRT, coordination with others, and so forth.

(c) The chief information security officer shall establish a reporting system through which all concerning parties immediately report to him or her in the event of security information incident.

(d) The chief information security officer shall designate employees who are in charge of CYMAT (this is only for national administrative organs).

(8) The roles that should not be concurrently undertaken by the same person

(a) Employees shall not concurrently undertake the following roles when implementing information security measures.

(i) A submitter of an application for approval or permission (hereinafter referred to as "approval, etc." in this paragraph), and a person authorized to give permission who approves the application
(ii) An auditee and an auditor

(b) When applying for approval, etc., if employees themselves are the persons authorized to give permission, or if it is irrelevant for such persons to decide whether the application should be approved or denied, such approval, etc. should be submitted to, and granted by, their supervisors or other parties deemed relevant.

2.1.2 Asset management

Purpose

It is important for Agencies to understand the state of their assets when considering information security measures. Insufficient understanding of assets may lead to unimplemented measures due to undetected assets and persistent threats in information systems that remain unattended. Furthermore, in the event of an information security incident, information collection to respond to the incident may take time if assets are not correctly managed, therefore leading to delayed response to the incident.
For this reason, Agencies must organize the information to understand the full picture of the assets of the respective organizations and maintain an information system ledger as an asset ledger so as to help their employees understand the assets.

Compliance Requirements

(1) Maintenance of the information system ledger
(a) The head information security officer shall maintain the information system ledger, recording all matters related to the security requirements of each information system.

2.1.3 Formulation of information security rules

Purpose

In order to appropriately maintain the level of information security at Agencies and comprehensively reduce information security risks, it is important to both establish standards for the measures with which Agencies should comply and systematically implement measures based on the results of risk assessments of information security.
It is necessary to establish specific operational rules and operating procedures to implement the measures set forth in the government agency's own standards. If they are not established or fully established, there is a risk of measures not being properly implemented. As such, it is important for the chief information security officer to instruct the head information security officer to formulate operational rules, etc. and receive periodic reports on the results to accurately understand the situation.

Compliance Requirements

(1) Implementation of risk assessments

(a) In light of the purposes of the Agencies, the chief information security officer shall, upon considering the results of self-inspections, information security audits, and headquarters audits, assess risks by analyzing the likelihood of threats occurring in the information in possession and information systems used, as well as the possible losses from such threats.

(2) Establishment of the government agency's own standards

(a) The chief information security officer shall establish the standards conforming to the Common Standards for Measures, so as to enable information security measures at least equivalent to those specified in the Common Standards, through deliberation by the Information Security Committee. In addition, they shall establish standards based on the results of risk assessments related to the Agency's work, the information it handles, and the information systems in its possession, as well as the results of reviewing the government agency's own standards and the measures promotion plan.

(3) Formulation of operational rules and operating procedures

(a) The head information security officer shall establish operational rules (excluding cases where the chief information security officer should establish such rules as per these Common Standards) and operating procedures (excluding cases where another person is designated to establish such procedures as per these Common Standards) for information security measures for Agencies. The head information security officer shall also direct tasks related to the operational rules and operating procedures, and report to the chief information security officer on the state of establishment of these rules and procedures.

(b) The head information security officer shall establish operational rules concerning information security measures on the start and end of employment and personnel reassignment.

(4) Establishment of the measures promotion plan

(a) The chief information security officer shall establish a measures promotion plan through deliberation by the Information Security Committee.

2.2 Operation

2.2.1 Enforcement of information security rules

Purpose

It is necessary for Agencies to properly enforce specific operational rules and operating procedures established to implement the measures stipulated in the government agency's own standards.

For the enforcement of information security rules, it is important to understand the issues and problems with these rules in addition to the state of their enforcement, in a timely manner.

Compliance Requirements

(1) Operation of information security measures

(a) The information security measure promotion structure shall carry out the necessary tasks according to the roles that have been designated for it by the chief information security officer.

(b) The information security officers or division/office information security officers shall report to the head information security officer, if there are any issues or problems with information security related provisions reported by employees.

(c) The head information security officer shall determine the application status regarding information security-related rules and regulations, including any issues or problems for this, in a timely manner and report the details of this to the chief information security officer as needed.

(2) Handling violations

(a) Employees shall report to the information security officers when they become aware of any serious breach of information security related provisions.

(b) The information security officers shall instruct the violator and concerned parties to take necessary measures to maintain information security when he or she is informed of, or becomes aware of any serious breach of information security related provisions, and shall report to the chief information security officer through the head information security officer.

2.2.2 Exceptional measures

Purpose

As exceptional measures are used only in case of exception, they should not be overused. However, there may be situations where employing methods other than those prescribed, or not implementing the prescribed measures should be approved, due to the reasons such as applying certain information security related provisions shall significantly hinder appropriate execution of administrative tasks. To handle such situations, it is necessary to establish procedures for exceptional measures.

Compliance Requirements

(1) Maintenance of exceptional measures

(a) The chief information security officer shall designate a person who examines and permits applications for exceptional measures (hereinafter referred to as “the permission authority” in this provision) and shall establish the examination procedure.

(b) The head information security officer shall maintain the records of exceptional measure application and request the permission authority to regularly report on application status.

(2) Operation of exceptional measure

(a) Employees shall follow the stipulated examination procedures when submitting applications for exceptional measures to the permission authority. In case that a task should

be executed immediately and can be handled with utmost respect for provisions, where taking measures other than those prescribed in the information security related provisions or not taking prescribed measures is unavoidable, applications for such exceptional measures shall be promptly submitted afterwards.

(b) The permission authority shall examine applications for exceptional measures submitted by employees in accordance with the stipulated approval procedures and determine whether or not to approve.

(c) The permission authority shall establish records of exceptional measure application and report them to the head information security officer.

(d) The head information security officer shall review information security measures for necessary revisions or additions based on the application status of exceptional measures, and report them to the chief information security officer.

2.2.3 Education

Purpose

Even when the information security related provisions are appropriately maintained, the level of information security cannot be enhanced if employees are not aware of, nor comply with their contents. Therefore, it is essential to educate all employees to let them acquire deeper knowledge of the information security rules.

It is necessary to bring up skilled human resources with expertise in information security for the reason of recent increase of information security incidents in Agencies and so forth.

Compliance Requirements

(1) Establishment of structures for information security measures education and formulation of education implementation plans

(a) The head information security officer shall establish education plans on information security measures based on the measures promotion plans, and maintain their enforcement framework.

(b) The head information security officer shall revise the education implementation plans in the event that matters on which education should newly be provided to employees come to light according to changes in the information security environment.

(2) Enforcement of information security measures education

(a) The division/office information security officer shall ensure employees duly participate in the education concerning information security-related regulations based on the education implementation plan.

(b) Employees shall duly participate in information security measure education, according to the education plan.

(c) The division/office information security officer shall ensure officers affiliated to the information security measure promotion structure and CSIRT duly participate in

information security measure education. In addition, division/office information security officers at national administrative organs shall ensure that employees affiliated with CYMAT properly receive information security measure education.

(d) The division/office information security officer shall record the information security measure education implementation status and report this to the information security officer and head information security officer.

(e) The head information security officer shall analyze and assess the information security measure education implementation status and report to the chief information security officer on the enforcement status of information security measures education.

2.2.4 Handling of information security incidents

Purpose

If an information security incident is detected, it should be immediately reported to the chief information security officer, and the measures to prevent the spread of damage as well as for recovery, should be implemented. Also, after handling the incident, it is important to identify the lessons to be learned by investigating the root causes, and utilize those lessons to prevent recurrence, and to review the systems and procedures.

Compliance Requirements

(1) Preparation for information security incidents

(a) The head information security officer shall establish/maintain reporting procedures, including points of contact within the Agencies in the event of information security incidents (including potential incidents), and shall inform all employees of these procedures including examples of reporting.

(b) The head information security officer shall establish/maintain procedures for measures including sharing information with parties other than Agencies in the event of information security incidents (including potential incidents).

(c) In preparation for information security incidents, the head information security officer shall establish an emergency communication network containing emergency contacts, communication methods, and contents to report, for the information systems deemed especially critical to execute administrative tasks.

(d) The head information security officer shall examine the necessity of education on measures against information security incidents, and establish/maintain the contents and framework of the education for the information systems deemed especially critical to execute administrative tasks.

(e) The head information security officers shall establish/maintain points of contact to receive reports on information security incidents from parties other than Agencies, and show them the method to communicate with such point of contact.

(f) The head information security officers shall confirm that the procedures for measures work adequately, through education and so forth.

(2) Handling of information security incidents

(a) Employees shall report to the points of contact at Agencies and follow their instruction in the event of information security incidents (including potential incidents).

(b) The CSIRT shall check the reported information security incident (including potential incident) and verify whether or not it is an information security incident.

(c) The head CSIRT officer shall immediately report to the chief security officer in the event of information security incidents.

(d) The CSIRT shall provide the relevant information security officers concerning the information security incident with instructions or advice on emergency measures to prevent spread of damage and to recover from the incident. The CSIRT shall also review any possibilities of a similar information security incident occurring in another information system, and if necessary, instruct the relevant information system security officers to check their information systems.

(e) Information security officers shall implement appropriate measures based on procedures stipulated by Agencies, or on CSIRT instructions or advice, in the event of information security incidents against the information security system under their management.

(f) In the event of information security incidents affecting a shared government system, the information system security officers of the shared government system user agencies shall duly follow the operation and management rules for information security measures for shared government systems when implementing measures.

(g) In case that the detected information security incidents are cyber-attacks or likewise, CSIRT shall report to the police.

(h) The CSIRT shall be aware of handling status of the information security incident and provide with instructions or advice on handling.

(i) The CSIRT shall record the handling of the information security incident.

(j) The CSIRT shall provide necessary information to CYMAT when receiving their supports.

(3) Sharing information on information security incidents

(a) When a CSIRT in a national administrative agency becomes aware of an information security incident in the information system of the agency, it shall promptly notify the National center of Incident readiness and Strategy for Cybersecurity. Additionally, if the CSIRT of the incorporated administrative agencies and designated corporations becomes aware of an information security incident in the information system of the agencies, it shall promptly notify the government agency that has jurisdiction over the relevant corporation regarding the incident. The CSIRT in a national administrative agency that receives this notification shall promptly contact the National center of Incident readiness and Strategy for Cybersecurity regarding the incident.

(b) In case that the information security incident recognized or contacted by the incorporated administrative agencies and designated corporations has caused or is likely to cause serious damage to the lives, bodies, property, or national territory of citizens and is a large-scale

cyber attack situation or the possibility of such a situation, a report and communication based on the Initial Response to Large-Scale Cyber Attack Situations (determined by Cabinet Crisis Management Supervisory Approval of March 19, 2010) shall be made.

(c) The CSIRT shall share information with the related agencies, including government agencies, regarding information security incidents.

(d) Any leakage of personal information or specific personal information due to an information security incident shall be reported to the Personal Information Protection Commission as necessary.

(4) Prevention of recurrence of information security incidents and sharing of lessons learned

(a) Information security officers shall, upon receiving instructions or advice from CSIRT on emergency measures and recovery, investigate the cause of information security incidents based on such instructions or advice, and review the measures for prevention and report them to the chief information security officer.

(b) The chief information security officer shall examine the report on information security incidents submitted by information security officers, and take necessary measures to prevent recurrence.

(c) The head CSIRT officer shall share the lessons learned from consequences of the incident handling with the head information security officer, the relevant information security officers and so forth.

2.3 Assessment

2.3.1 Self-check of information security measures

Purpose

To ensure effectiveness of information security measures it is vital to assess how the information security related provisions are complied with, and to analyze the results of such assessments.

It is important to appropriately carry out self-check to see if an employee duly carries out the measures implemented according to his or her role, and also to assess the level of information security in the entire Agency.

In addition, it is important for each concerning party to implement the necessary revised measures within the scope of his or her responsibility for the role, based on the results of self-check.

Compliance Requirements

(1) Formulation of self-check plans and establishment of procedures

(a) The head information security officer shall formulate an annual plan for self-checks based on the measures promotion plan.

(b) Information security officers shall maintain self-check forms and procedures for each employee based on the annual plan for self-checks.

(c) The head information security officer shall revise the annual plan for self-checks in the event that matters that should be newly checked come to light according to changes in the information security environment

(2) Conducting self-check

(a) Information security officers shall instruct employees to conduct self-check in accordance with the annual self-check plan.

(b) Employees shall conduct self-check using the self-check forms and procedures prepared by information security officers.

(3) Evaluations and improvements based on self-check

(a) The information security officers shall analyze and evaluate the results of the self-checks in the interest of confirming whether there are any problems unique to the Agency they oversee as a whole. They shall also report the evaluation results to the head information security officer.

(b) The head information security officer shall analyze and evaluate the results of the self-checks in the interest of confirming whether there are any problems commonly shared throughout the Agency. They shall also report the evaluation results to the chief information security officer.

(c) The chief information security officer shall evaluate the overall results of self-check and instruct information security officers to make improvements on any identified issues. The chief information security officer shall be reported concerning the results of improvements.

2.3.2 Information security audit

Purpose

To ensure effectiveness of information security measures it is also vital to ensure that an independent party to carry out information security audit, while parties engaged in information security measures to conduct self-check. Information security audits conducted by Agencies enable better understanding of operations and information systems, as well as efficient in-depth investigations, and are also important for the smooth functioning of the PDCA cycle for the improvement of the respective organizations' information security measures.

In addition, it is important for the chief information security officer to instruct information security officers to implement necessary measures based on the issues identified by the audit.

Compliance Requirements

(1) Formulation of audit plans

(a) The head information security auditor shall formulate plans for information security audit based on the promotion plan of measures.

(b) The head information security auditor shall establish an additional audit implementation plan in case it is necessary to perform an audit that is not defined in the promotion plan of measures, responding to situational changes in information security.

(2) Conducting information security audit

(a) The head information security auditor shall instruct information security auditors to conduct audits in accordance with the promotion plan of measures, and provide the chief security officer with an audit report.

(3) Responding to audit results

(a) The chief information security officer shall instruct the head information security officer and information security officers to formulate improvement plans for any issues pointed out in the audit report. For any improvement plans whose implementation is not completed, the chief information security officer shall give instructions to periodically report on the progress.

(b) The head information security officer shall formulate improvement plans after first taking the necessary measures for items requiring cross-sectoral improvements within the Agency from among those for which the chief information security officer has requested improvements. They shall also report the results of the measures taken and the improvement plans to the chief information security officer. For any improvement plans whose implementation is not completed, the head information security officer shall periodically report the progress to the chief information security officer.

(c) The information security officers shall, after taking the necessary measures, formulate improvement plans for the issues requiring specific improvements for the Agencies they oversee as a whole from among those for which the chief information security officer has requested improvements. The information security officers shall report the results of taking the necessary measures and the improvement plans to the chief information security officer. For any improvement plans whose implementation is not completed, the information security officers shall periodically report the progress to the chief information security officer.

2.4 Review

2.4.1 Review of information Security measures

Purpose

As the environment surrounding information security is constantly changing, the level of information security cannot be maintained if these changes are not appropriately addressed. Therefore, it is necessary to conduct periodical reviews on the information security related provisions which serve as the basis for information security measures for Agencies. At that time, it is essential to assess risks by analyzing potential threats and damages in case of their occurrence concerning possessed information

and information systems, taking into account the matters such as issues with actual operations, results of self-inspections and audits, and change of circumstances surrounding information security.

It is also vital to reflect these results in the standards and promotion plan of measures to further promote the initiatives for information security.

Compliance Requirements

(1) Review of information security measures

(a) Whenever there is a change in the risk assessment, the chief information security officer shall, upon deliberation by the Information Security Committee, review and revise the government agency's own standards and the measures promotion plans as necessary.

(2) Review of information security rules, etc.

(a) The chief information security officer shall comprehensively evaluate the information security operation and the results of self-checks, as well as information security audits and headquarters audits, and conduct a necessary review on the government agency's own standards, taking into account the significant situational changes in information security, and after deliberations of the Information Security Committee.

(b) The head information security officer shall review the information security operational rules and operating procedures, taking into account the information security operations and the results of self-checks, as well as information security audits and headquarters audits, or shall instruct who prepared the procedures to review the provisions, and report the results to the chief information security officer.

(c) Based on the information security operation and the results of self-checks, as well as information security audits and headquarters audits, the head information security officer shall take action according to the roles and duties within the Agency for the review and revision of information security measures that have been found to need improvement throughout the Agency, or shall instruct another person to take such action. The head information security officer shall then report the results of such action to the chief information security officer.

(3) Review of promotion plan of measures

(a) The chief information security officer shall comprehensively evaluate the information security operation and the results of self-checks, as well as information security audits and headquarters audits, and conduct a necessary review on the measures promotion plan, taking into account the significant situational changes in information security, and after deliberations of the Information Security Committee.

2.5 Incorporated Administrative Agencies and Designated Corporations

2.5.1 Information security measures for incorporated administrative agencies and designated corporations

Purpose

Some incorporated administrative agencies and designated corporations may handle information that falls under important information of government agencies, in which case information security measures must be properly implemented likewise those at government agencies. To that end, it is important for the information security management to properly function through coordination with the government agency that has jurisdiction over the relevant corporation.

Compliance Requirements

(1) Development of a structure in the government agency that has jurisdiction over the relevant incorporated administrative agencies and designated corporations

(a) The chief information security officer of the government agency that has jurisdiction over the relevant incorporated administrative agencies and designated corporations shall give instructions to develop a necessary system within the Agency for properly promoting information security measures of the relevant incorporated administrative agencies and designated corporations.

(2) Information security measures by incorporated administrative agencies and designated corporations

(a) The chief information security officers of incorporated administrative agencies and designated corporations shall, for the purpose of properly promoting information security measures, seek advice from the government agency that has jurisdiction over that incorporated administrative agency or designated corporation regarding matters that require close coordination with the relevant government agencies and matters that need expert opinions.

Chapter 3 Information Handling

3.1 Information Handling

3.1.1 Information handling

Purpose

The execution of work requires information handling such as preparation, obtainment, use, storage, provision, transportation, transmission, and deletion (hereinafter referred to as "use or handling" in this provision). In order to maintain the security of certain information, all employees who use or handle such information need to implement appropriate measures corresponding to its characteristics at each phase of the information lifecycle. For this reason, it is necessary for employees to take actions such as labeling classifications and handling restrictions of information upon its preparation or obtainment, to share the same understanding on handling of such information, as well as to implement measures in accordance with its classification and handling restrictions.

The Document Management Guidelines shall be primarily applied for management of confidential documents at national administrative organs. For the matters related to information security measures not stipulated in the Guidelines, it is essential to ensure appropriate information handling based on the Common Standards. In addition, measures shall be taken based on the provisions of these Common Standards regarding the management of confidentiality class-3 information at Incorporated Administrative Agencies and Designated Corporations.

Compliance Requirements

(1) Maintenance of provisions related to information handling
   (a) The head information security officer shall maintain the operational rules on information handling which contains all of the following items and notify them to employees.
      (i) Definitions of "classifications and handling restrictions of information"
      (ii) Procedures of labeling, etc. of "classifications and handling restrictions of information"
      (iii) Procedures of maintenance and review of "classifications and handling restrictions of information"

(2) Prohibition of use or handling of information for non-job related purposes
   (a) Employees shall limit the use or handling of the information within the scope of their job functions.

(3) Determination and labeling, etc. of classifications and handling restrictions of information
   (a) When preparing information or start managing information prepared by parties other than Agencies, employees shall determine the classifications and handling restriction of information in accordance with its definitions, and take necessary actions of labeling, etc.
   (b) When preparing or duplicating information, employees shall maintain the same confidentiality classification and handling restrictions as the original, if the obtained or referred original information is already classified according to its level of confidentiality.

(c) If the existing classifications and handling restrictions deem necessary to be reviewed for amendments, additions, deletions, and for other reasons, employees shall consult with a person, or his or her senior, who determines the classifications and handling restrictions (including those who follow the determination- hereinafter referred to as the "classifying authority in this section), and conduct reviews based on the outcome of such consultation.

(4) Use and storage of information

(a) Employees shall appropriately handle information in accordance with the classification and handling restrictions, which is labeled, or otherwise specified.

(b) Employees shall obtain permission from their division/office information security officers when processing confidentiality class-3 information outside of the areas requiring control measures.

(c) Employees shall take necessary security management measures when processing classified information outside of the areas requiring control measures.

(d) Employees shall appropriately manage information in accordance with the classification and handling restrictions of information, such as setting access control when saving information. The employees of Incorporated Administrative Agencies and Designated Corporations shall take the following steps when storing confidentiality class-3 information to devices. However, when confidentiality class-3 information is handled in a manner equivalent to national administrative organs by Incorporate Administrative Agencies and Designated Corporations, their employees may take steps equivalent to those taken by national administrative organs in lieu of the following steps.

(i) When storing confidentiality class-3 information to devices, devices such as terminals, servers, and so on that are not connected to the internet or information systems with internet connections must be used.

(ii) The said information must be stored in an encrypted state.

(iii) Measures must be taken to protect the devices on which the said information is stored from physical threats, such as theft or their unauthorized removal.

(e) Employees shall follow the prescribed procedures when handling information using external storage media, such as USB memories and so on.

(5) Provision and disclosure of information

(a) When disclosing information, employees shall make sure the information is classified as class 1 information.

(b) When providing information to parties outside of the scope of viewing restrictions, employees shall consult with the classifying authority and follow his or her decision. In addition, employees shall ensure that the information is properly handled in accordance with the prescribed classification and handling restrictions at the parties' sites. To achieve

this employees shall take measures such as to assuredly inform the parties of points to be noted when handling such information.

(c) When providing confidentiality class-3 information to parties outside of the scope of viewing restrictions, employees at Incorporated Administrative Agencies and Designated Corporations shall receive the approval of their division/office information security officer.

(d) When providing or disclosing information in electronic or magnetic format, employees shall take measures to prevent inadvertent information leakage.

(6) Transportation and transmission of information

(a) When transporting an external storage media which stores or contains classified information to places outside the areas requiring control measures, employees shall select the means of transportation with considerations to security and take appropriate measures to ensure security in accordance with the classification and handling restrictions of the information. When the employees of Incorporated Administrative Agencies and Designated Corporations take confidentiality class-3 information outside of areas requiring control measures, this is to be transported via the method specified by the division/office information security officer after first encrypting the information. In case that the media is transported only to an area pre-designated by the head security officer, which is defined as the areas requiring handling restrictions by other Agencies, such an area shall be regarded as an area requiring control measures.

(b) When transmitting classified information in electronic or magnetic format such as e-mail, employees shall select the means of transmission with considerations to security, and take appropriate measures to ensure security in accordance with the classification and handling restriction of information. When the employees of Incorporated Administrative Agencies and Designated Corporations use communication lines outside the Agency (excluding the internet) to transmit confidentiality class-3 information, they shall transmit this via the method specified by the division/office information security officer after first encrypting the information. However, when confidentiality class-3 information is handled in a manner equivalent to national administrative organs by Incorporate Administrative Agencies and Designated Corporations, their employees may take steps equivalent to those taken by national administrative organs in lieu of the above action.

(7) Deletion of information

(a) Employees shall immediately erase the information stored in an external storage media when it becomes unnecessary for their job functions.

(b) When disposing of an external storage media, employees shall erase all the information stored, making it completely unrestorable and ensuring there is no remaining information in the media.

(c) When disposing of confidential information in written format, employees shall make it unrestorable.

(8) Backup of information

(a) Employees shall take backup of information in an appropriate manner in accordance with the classification of information.

(b) Employees shall determine the place, manner, period for storage and so on, of the backup information, and appropriately manage it in accordance with the classification and handling restriction of information.

(c) Employees shall appropriately delete, erase or dispose of the information with exceeded storage period, in accordance with the provisions set forth in the previous section.

3.2 Information Handling Areas

3.2.1 Information handling areas

Purpose

When the server equipment, terminals and other equipment are installed in an environment physically accessible by unspecified large number of publics, there are risks such as malicious impersonation, physical destruction to the equipment, and information leakage caused by illegal removal of such equipment. Other threats concerning the environment where the systems are installed include damage to information systems as a result of disasters.

Therefore, it is necessary to ensure security of information and information systems in the areas including offices, conference rooms, and server rooms where information is handled, by implementing measures such as physical countermeasures, as well as entrance and exit management systems, and so on.

Compliance Requirements

(1) Determine the standards for measures for the areas requiring control measures

(a) The head information security officer shall determine the scope of the areas requiring control measures.

(b) The head information security officer shall establish, as operational rules, the standards for measures for the areas requiring control measures according to the characteristics of each area which include all of the following items.

(i) Physical measures to prevent easy access to the areas by unauthorized persons, including maintenance and installation of facilities such as lockable doors and partitions.

(ii) Entrance and exit management systems to restrict unauthorized persons to enter the areas, as well as to prevent illegal actions by authorized persons while they are in the areas.

(2) Determine the measures to be implemented in each area

(a) Information security officers shall determine areas per unit where they implement measures for facilities and work environments based on the standards set forth by the head information security officer.

(b) Area information security officers shall determine measures to be implemented in the areas they manage, considering the matters such as the standards set forth by the head information security officer, surrounding environment, type of administrative tasks, and information handled in such areas.

(3) Implementation of measures for the areas requiring control measures

(a) Area information security officers shall implement measures determined in the areas they manage. As for the measures need to be carried out by employees, area information security officers shall take actions to ensure that employees duly understand and recognize such measures.

(b) Area information security officers shall implement physical measures to protect information systems which handle vital information from disasters.

(c) Employees shall use the areas in accordance with the measures determined by area information security officers. Employees shall ensure those who belong to parties other than their own Agencies use the areas in accordance with the prescribed measures when allowing such external parties to enter the areas.

Chapter 4 Outsourcing

4.1 Subcontracting

4.1.1 Subcontracting

Purpose

When operations such as research and survey, or the development, operation, or maintenance of information systems or application programs, are contracted out to external parties which makes it difficult for employees to directly manage the information security measures at the subcontractors, it would be vital to specify requirements for subcontractors in documents such as procurement specifications and include them in terms of contracts, in order to ensure the information security measures for properly protecting confidential information that is provided to subcontractors are duly implemented by subcontractors.

There are a variety of forms of subcontracting as shown in the examples below, and forms of agreement vary from fixed-price contracts, delegation contracts and semi-delegation contracts to consent to general terms and conditions, and so on. In any case where an agreement is entered into for subcontracting tasks for which it is necessary that information security measures for properly protecting confidential information that is provided to subcontractors are duly implemented by subcontractors as stated above, it is important to clearly define the scope of tasks contracted out and responsibilities incurred by subcontractors, and to reach a mutual agreement on details of information security measures.

In cases where the subcontracted operation uses a cloud service, the provisions of section 4.2 “Use of Cloud Services” shall also be included in the requirements for the subcontractor according to the classification of the handled information, operations subcontracted, and the nature of the cloud service used, since the subcontractor would also be exposed to risks specific to cloud services. When subcontracting an operation that concerns an information system, since there are different risks specific to information systems, the provisions of section 4.1.2 “Subcontracting that involves an information system” must also be implemented. When procuring equipment, etc., since there are risks in the supply chain of the equipment, etc. to be procured, the provisions of section 4.3 “Procurement of Equipment, etc.” must also be implemented.

<Examples of operations subcontracted>

- Development and construction of information systems
- Development of applications and contents, and so on.
- Operation of information system
- Operation support services (statistics, data aggregation, data entry, media conversion, and so on.)
- Project management support services
- Investigation and research (investigation, research, examination, etc.)
- Operation of websites

Compliance Requirements

(1) Maintenance/establishment of operational rules related to subcontracting

(a) The head information security officer shall maintain/establish operational rules related to subcontracting which include all of the following items.

(i) Criteria for determining the scope of information that may be provided to subcontractors and the operations subcontracted (hereinafter referred to as the "criteria and procedures for selection" in this provision).

(ii) Criteria and procedures for selecting subcontractors.

(2) Measures taken before subcontracting

(a) Information system security officers or division/office information security officers shall perform all of the following measures before subcontracting any operations.

(i) Identification of operations to be subcontracted

(ii) Formulation of subcontractor selection criteria and other specifications

(iii) Selection of subcontractor(s) based on specifications

(iv) Conclusion of agreement

(v) Conclusion of a non-disclosure agreement (NDA) if providing confidential information to the subcontractor

(b) Before subcontracting, information system security officers or division/office information security officers shall require subcontractors to perform all of the following as a prerequisite for subcontracting.

(i) Proposals in compliance with the specifications

(ii) Conclusion of agreement

(iii) Conclusion of a non-disclosure agreement (NDA) if the subcontractor is handling confidential information

(3) Measures during the subcontracting period

(a) Information system security officers or division/office information security officers shall perform all of the following measures during the subcontracting period.

(i) Provision of confidential information in accordance with the criteria and procedures for selection

(ii) Periodic check of the implementation of information security measures that are performed by subcontractors based on agreement

(iii) In the event of information security incidents or use of information for purposes aside from those specified for the subcontracted operation, or any report thereof from an employee, request for action based on agreement, including suspension of subcontracted operations and other necessary measures

(b) Information system security officers or division/office information security officers shall require subcontractors to implement all of the following measures during the subcontracting period.

(i) Information security measures for proper handling of information
(ii) Periodic report on the implementation of information security measures that are performed by subcontractors based on agreement
(iii) In the event of information security incidents or use of information for purposes aside from those specified for the subcontracted operation, or any report thereof from an employee, measures such as suspension of subcontracted operations

(4) Measures at the completion of subcontracting
(a) Information system security officers or division/office information security officers shall perform all of the following measures at the completion of subcontracting.
(i) Inspection involving confirmation of proper implementation of security measures throughout the subcontracting period
(ii) Confirmation that information handled by the subcontractor, including information provided to the subcontractor, has been returned, discarded, or erased
(b) Information system security officers or division/office information security officers shall require subcontractors to implement all of the following measures at the completion of subcontracting based on agreement.
(i) Report on and cooperation in inspections to confirm that security measures have been properly implemented throughout the subcontracting period
(ii) Return, disposal, or erasure of information handled by the subcontractor for the subcontracted operations, including information provided to the subcontractor

4.1.2 Subcontracting that involves an information system

Purpose

When subcontracting operations concerning information systems, such as the development, operation, and/or maintenance of information systems or application programs, to non-Agency entity, the following must be set forth in procurement specifications as requirements to the subcontractor and be included in the terms of contracts: measures taken to prevent any changes unintended by the Agency from being made to the information systems by the subcontractor in addition to the provisions in 4.1.1 "Subcontracting," and in the development, operation, or maintenance phase of an information system, specific measures that must be implemented for subcontracting operations concerning information systems, such as measures to prevent vulnerabilities.

<Examples of subcontracted operations involving information systems>

- Development and construction of information systems
- Development of applications and contents
- Operation of information system
- Operation of the common platform system used only within Agencies (information system that provides a platform that shares a part or all of the resources and software of information systems) (hosting private cloud)

Compliance Requirements

(1) Common measures for subcontracting involving an information system

(a) Before subcontracting any operation involving an information system, information system security officers shall formulate specifications upon adding, to the subcontractor selection criteria, the selection criteria concerning measures to prevent any changes unintended by Agencies from being made to the information system.

(2) Measures for subcontracting the construction of an information system

(a) When subcontracting the construction of an information system, information system security officers shall oblige the subcontractor to implement all of the following measures based on agreement.

(i) Proper implementation of security requirements for the information system

(ii) System tests conducted from perspectives of information security

(iii) Information security measures in the development environment and process of the information system

(3) Measures for subcontracting the operation and maintenance of an information system

(a) When subcontracting the operation and maintenance of an information system, information system security officers shall, based on agreement, require the subcontractor to implement the requirements for proper operation of security functions implemented in the information system.

(b) When subcontracting the operation and maintenance of an information system, information system security officers shall, for the purpose of properly understanding the information security measures implemented by the subcontractor for the information system, based on agreement, require the subcontractor to promptly report on any changes to the information system made by the measures.

(4) Measures for using services that provide some functions of the information system to Agencies

(a) When subcontracting for an information system in order to allow non-Agencies to use a service that provides Agencies with some functions of an information system that handle confidential information (excluding cloud services) (hereinafter referred to as "subcontracted service"), information system security officers or division/office information security officers shall add, to the subcontractor selection criteria, the selection criteria specific to the subcontracted service.

(b) Information system security officers or division/office information security officers shall select subcontracted services upon establishing security requirements for subcontracted services.

(c) Information system security officers or division/office information security officers shall comprehensively and objectively evaluate and determine whether the subcontractor is sufficiently reliable.

(d) When using a subcontracted service, information system security officers or division/office information security officers shall make an application to use the service to the head information security officer or information security officers.

(e) When the head information security officer or an information security officer receives an application for using a subcontracted service, the officer shall review the application and decide whether or not to allow the use of the service.

(f) If the head information security officer or the information security officer approves the application for using the subcontracted service, the officer shall record it as an approved subcontracted service and assign an administrator for the subcontracted service.

4.2 Use of Cloud Services

4.2.1 Selection of cloud services to handle confidential information

Purpose

Information whose handling is entrusted by Agencies to subcontractors should be handled appropriately by the subcontractors. However, it is not generally easy to confirm directly the details of security measures implemented in cloud services. Therefore, when an Agency handles confidential information using a cloud service, it is necessary to understand the characteristics of the cloud service, fully consider matters necessary for ensuring security in the use and the effectiveness of governance to the cloud service provider by the Agency, clarify roles and responsibilities shared between the Agency and the cloud service provider, and then ensure that the cloud service meets selection criteria and security requirements.

<Examples of cloud services>

- Services that provide a virtual server, storage, hypervisor, etc. (IaaS)
- Services that provide middleware such as database and development framework (PaaS)
- Web conference services
- Social media
- Search services, translation services, mapping services

In most of cases of cloud services that are provided by private service providers to an unspecified number of users and become available only on consent to standard general terms and conditions, terms of services, etc., it is impossible to request that those providers take security measures or handle data in a special manner for Agencies, and it is generally difficult to satisfy necessary and sufficient security requirements for the handling of confidential information. Therefore, in principle, handling of confidential information in this type of cloud services is not allowed, and the provisions in 4.2.3 “Selection and use of cloud services to handle non-confidential information only” must be followed.

Compliance Requirements

(1) Maintenance/establishment of operational rules related to the selection of cloud services

(a) The head information security officer shall establish/maintain operational rules related to the selection of cloud services (in cases where confidential information is handled), including all of the following items.

(i) Criteria on types of tasks and information systems to allow use of cloud services, and on location restrictions for handling confidential information (hereinafter referred to as the "Criteria for Allowing Use of Cloud Services" in this section 4.2)
(ii) Criteria for selecting cloud service providers
(iii) Permitting authority and procedures for starting use of cloud services
(iv) Designation of the cloud service administrator and management of use of each cloud service

(2) Selection of cloud services
(a) Information system security officers or division/office information security officers shall review the use of cloud services while taking into account the classification of and handling restrictions on information to be handled, as well as the impact on operations, in accordance with the Criteria for Allowing Use of Cloud Services.
(b) Information system security officers or division/office information security officers shall establish security requirements including all of the following while taking into account the classification of and handling restrictions on information to be handled, as well as the scope of roles and responsibilities of the cloud service provider regarding information security.
(i) Information security measures required for the cloud service
(ii) Country/Region where the information handled in the cloud service is saved and the method of disposal
(iii) Service level required for the cloud service
(c) Information system security officers or division/office information security officers shall, in accordance with the selection criteria for cloud services, select cloud services from a cloud service list such as ISMAP in principle in light of the security requirements established as described in the preceding paragraph.

(3) Procurement for use of cloud services
(a) In cases of procurement of cloud services, information system security officers or division/office information security officers shall include in procurement specifications the criteria and terms of selection of cloud service providers as well as security requirements established upon selection of cloud services.
(b) In cases of procurement of cloud services, information system security officers or division/office information security officers shall confirm that the cloud service provider and its services meet procurement specifications before concluding the agreement, obtain approval for the use of the service, and have an agreement with the provider include the procurement specifications.

(4) Approval for use of cloud services

(a) In cases of use of cloud services, information system security officers or division/office information security officers shall submit applications for use of cloud services to the person authorized to permit use applications.

(b) The person authorized to permit use applications shall examine use applications for cloud services as described in the preceding paragraph, and decide whether or not to use the services.

(c) The person authorized to permit use applications shall, when approving use applications for cloud services, keep records of approved cloud services and designate the cloud service administrator.

4.2.2 Use of cloud services to handle confidential information

Purpose

It is necessary to take security measures in using cloud services not only when cloud service providers are selected and agreements are entered into with the providers, but also when information systems using the cloud service are introduced and constructed after the agreements are entered into with the providers, and then operated and maintained, and furthermore, throughout the lifecycle of the relevant information system until the termination of its agreement.

The content of each cloud service is changing at a very rapid pace, and it is possible to streamline operations and improve information security by utilizing the newly added functions. On the other hand, threats and vulnerabilities that were not anticipated as of the construction of the information system may arise. Therefore, it is required to thoroughly add and modify security requirements through review by periodically checking the information security measures in using cloud services. For access rights to cloud services, it is also important to conduct review by periodically checks according to the changes in the operations of Agencies and/or usage environment of cloud services.

This section specifies information security measures that are particularly necessary at each phase in the life cycle when using a cloud service. For information security measures necessary at each phase in the life cycle of the entire information system, additional compliance with the provisions in 5.2 “Measures at Each Phase of Information System Lifecycle” is required.

Compliance Requirements

(1) Establishment/Maintenance of operational rules for using cloud services

(a) Based on the nature of the cloud service and concept of the demarcation point of responsibilities, the head information security officer shall establish/maintain, as operational rules, the basic policy for security measures when introducing and constructing an information system using a cloud service.

(b) Based on the nature of the cloud service and concept of the demarcation point of responsibilities, the head information security officer shall establish/maintain, as operational rules, the basic policy for security measures when operating and maintaining an information system using a cloud service.

(c) Based on the nature of the cloud service and concept of the demarcation point of responsibilities, the head information security officer shall establish/maintain, as operational rules, the basic policy for security measures including all of the following when ending the use of a cloud service.
  (i) Measures when ending the use of a cloud service
  (ii) Disposal of information handled in a cloud service
  (iii) Disposal of accounts created for using a cloud service

(2) Formulation of security requirements for using cloud services
  (a) Based on operational requirements, including the purposes of use of the cloud service and the relevant operations, as well as the classification of information handled in the cloud service, cloud service administrators shall confirm the details on the use of the cloud service according to the operational rules as basic policy established in the items under (1).
  (b) Based on operational requirements, including the purposes of use of the cloud service and the relevant operations, as well as the classification of information handled in the cloud service, cloud service administrators shall formulate security requirements for the use of the cloud service according to the operational rules as basic policy established in the items under (1).

(3) Measures when introducing or constructing an information system using a cloud service
  (a) Based on the operational rules set forth as per (1)(a), cloud service administrators shall take necessary measures for using the cloud service in accordance with the security requirements established as per (2)(b). The cloud service administrators shall also confirm and record the status of such measures when introducing or constructing the information system.
  (b) When using a cloud service for an information system, cloud service administrators shall record or write in the information system ledger and relevant document(s), and make a report to the head information security officer.
  (c) Cloud service administrators shall establish all of the following operating procedures, as documents necessary for implementing information security measures for the cloud service, before the start of use of the cloud service.
    (i) Procedure for maintaining the information security level for each service used with the cloud service
    (ii) Procedure for handling any information security incidents detected while operating or monitoring the information system using the cloud service
    (iii) Procedure for recovery when the cloud service stops or becomes unavailable

(4) Measures when operating or maintaining an information system using a cloud service
  (a) Based on the operational rules set forth as per (1)(b), cloud service administrators shall properly perform the operation and maintenance for the cloud service. The cloud service administrators shall also periodically confirm and record the status of such operation and

maintenance.

(b) If a correction or a change occurs to an item necessary for implementing information security measures when operating or maintaining the cloud service, cloud service administrators shall update or correct the information system ledger and relevant document(s). Whenever the information system ledger is updated or corrected, make a report to the head information security officer.

(c) Cloud service administrators shall perform review and revision as necessary whenever a new threat emerges or according to the situation of operation, monitoring, etc. and take necessary information security measures for the cloud service.

(5) Measures when revising or discarding an information system using a cloud service

(a) Based on the operational rules set forth as per (1)(c), cloud service administrators shall take the necessary measures for revision or disposal. Cloud service administrators shall also confirm and record the status of implementation when ending the use of the cloud service.

4.2.3 Selection and use of cloud services to handle non-confidential information only

Purpose

Even if confidential information is not handled and the level of information management required for cloud service providers is not high, it is required that cloud services be used after full recognition that various information is sent from Agencies and a decision on whether or not to use them has been made in full consideration of risks. On the other hand, requirements for security measures equivalent to cases where confidential information is handled will hinder the promotion of use of cloud services. Therefore, in cases where cloud services are used on the premise that confidential information is not handled, it is required that information security measures be appropriately taken in accordance with Compliance Requirements set forth in this section.

Compliance Requirements

(1) Maintenance/establishment of operational rules related to use of cloud services when not handling any confidential information

(a) The head information security officer shall establish/maintain operational rules related to use of cloud services (in cases where confidential information is not handled), which include all of the following items.

(i) Scope of tasks for which cloud services are usable

(ii) Permitting authority and procedures for starting use of cloud services

(iii) Designation of the cloud service administrator and management of use of each cloud service

(iv) Operational rules for use of cloud services

(2) Implementation of measures for use of cloud services when not handling any confidential information

(a) When using a cloud service on the premise of not handling any confidential information, employees shall make sure that the risks of using cloud services are tolerable by checking the general terms and conditions and other terms of the services, and then apply to the person authorized to permit use applications for the use of such services in cases where confidential information is not handled.

(b) Based on the general terms and conditions of the cloud service and other terms of the service, upon confirming that the risks of using the cloud service are tolerable, the person authorized to permit use applications shall examine use applications for cloud services submitted by employees to determine whether or not to permit them.

(c) Upon approving a use application for a cloud service with no handling of confidential information, the person authorized to permit use application shall assign a cloud service administrator and record the approved cloud service.

(d) Cloud service administrators shall take appropriate measures for the safe use of the cloud service where no confidential information is handled.

4.3 Procurement of Equipment, etc.

4.3.1 Procurement of equipment, etc.

Purpose

Confidentiality, integrity and availability of information processed by information systems may be compromised if a procured equipment lacks required security functions, or any malicious alternation was made during its manufacturing process, or in those cases where information security measures cannot be continuously implemented to the procured equipment. Furthermore, information systems that incorporate equipment, etc. with unauthorized alteration can allow unauthorized access to the information systems, which may result in theft or destruction of confidential information and/or an information system failure.

To address these issues, it is necessary to establish/maintain criteria for selecting equipment etc., as well as procedures for checks and inspections at the time of delivery, to ensure the procurement is made in accordance with the government agency's own standards.

Compliance Requirements

(1) Establishment/Maintenance of operational rules for the procurement of equipment, etc.

(a) The head information security officer shall establish and maintain the selection criteria for equipment, etc. as operational rules. If necessary, a requirement for management that prevents any unauthorized alterations to the equipment, etc. during the lifecycle of such equipment (such management should be verifiable by Agencies), including its development phase, should be included in the selection criteria.

(b) The head information security officer shall establish and maintain the checks and inspection procedure for accepting delivery of equipment, etc. from the perspective of information

security measures.

Chapter 5 Lifecycle of Information Systems

5.1 Classification of Information Systems

5.1.1 Establishment of information system classification standards

Purpose

Amid the diversification of information systems managed by Agencies, in order to reduce the risks of information security incidents in information systems managed by the respective organizations, it is necessary to properly and sufficiently select measures required for the specific information systems from among the diverse range of information security measures.

To this end, based on the trend of information security threats, impact of information system security incidents on operations, social impact, information handled, and organizational characteristics of Agencies, it is important to enable proper measures to be taken according to the classification of the information systems managed by respective organizations by establishing classification standards to identify information systems that need a high level of information security measures and specifying information security measures according to the classification standards.

Compliance Requirements

(1) Establishment/Maintenance of operational rules for the classification of information systems

(a) Based on the operational impact of information security incidents occurring on an information system, the head information security officer shall establish and maintain information system classification standards, as operational rules, to identify information systems that need a high level of information security measures.

(2) Establishment/Maintenance of operational rules for information security measures based on the classification of information systems

(a) The head information security officer shall establish and maintain, as operational rules, the security requirements according to the classification standards for the information system and the specific items of information security measures for each component of the information system.

(3) Implementation of classification based on information system classification standards

(a) The head information security officer shall have information system security officers classify information systems based on the information system classification standards and have them report the classification results. For the results of the classification of information systems reported from information system security officers, the head information security officer shall, based on the operational impact of information security incidents and threat trend, give instructions to correct the classification if a higher or a lower class is more desirable for certain information systems.

(4) Review of operational rules for information system classification standards and specific items of information security measures

(a) The head information security officer shall review the operational rules for information system classification standards and specific items of information security measures according to the classification standards through periodic checks.

(b) The head information security officer shall periodically confirm that all information systems are properly classified according to the classification standards.

5.2 Measures at Each Phase of Information System Lifecycle

5.2.1 Planning and definition of requirements for information systems

Purpose

To appropriately maintain information security throughout the lifecycle of information system, it is necessary to define security requirements appropriately.

Ambiguous, excessive, or insufficient security requirements may result in disadvantages such as cost increase due to excessive measures for information security, unfair competitive biddings caused by different proposal contents due to widely varied interpretations of requirements, and rework in designing and development, as well as information security incidents after commencement of operations.

Therefore, it is important to review measures for expected threats against information systems and to appropriately include sufficient security requirements in specifications, after taking consideration of the scope of tasks, information handled, users who handle the information, as well as the environments and methods and so on used for information processing.

In addition, it is vital to examine the measures to protect the information systems to be constructed from vulnerabilities at the planning phase of the systems, before its construction.

It is also necessary to refer to 4.1 “Subcontracting” when subcontracting construction, operation, and maintenance of information systems, 4.2 “Use of Cloud Services” when constructing an information system using a cloud service, 4.3 “Procurement of Equipment, etc.” when procuring equipment, etc. to be used in an information system, and 5.4 “Shared Government Systems” when constructing an information system using a shared government system.

Compliance Requirements

(1) Ensuring the implementation of frameworks

(a) Information system security officers shall request that chief information security officers ensure the implementation frameworks, which enable them to maintain information security throughout the information system's lifecycle.

(b) When the cooperation of the person responsible for the management of information systems (chief digital officer (CIO)) must be obtained to ensure the frameworks required in the previous item, the chief information security officer shall request that said person responsible for the management of information systems set said frameworks in place in whole or in part.

(2) Implementation of classification based on information system classification standards

(a) When newly constructing or updating an information system, information system security officers shall classify the information system based on the information system classification standards and report it to the head information security officer.

(3) Formulation of security requirements for information systems

(a) Information system security officers shall formulate security requirements including all of the following items, taking into account matters such as purpose of constructing the information system, task requirements for the targeted tasks and so on, as well as classification of information handled by said system, based on the classification of the information system and the specific items of measures according to the classification standards required for the information system.

(i) Requirements for security functions to be incorporated to the system such as user/entity authentication, access control, authority control, log management, and encryptions

(ii) Requirements for operational management functions such as monitoring, while the information systems are in operation (if the data to be monitored has been encrypted, it must be decrypted as needed).

(iii) Requirements for measures against vulnerabilities and malicious programs of the information systems

(iv) Requirements for measures for the availability of the information system

(v) Requirements for the network configuration of the information system

(b) When constructing an information system connected to the internet, information system security officers shall decide the communication lines to connect and define security requirements for multiple protection to diminish risks of leakage, manipulation and so forth, caused through the internet such as targeted attacks.

(c) Information system security officers shall refer to the “List of Requirements for Ensuring Security in Procurement of IT Products” when procuring an equipment, and shall analyze the threats in the environments where the equipment is used, and formulate security requirements to counter the information security threats in said equipment, etc.

(d) For information systems that need a high level of information security measures in light of the information handled by the information system to be constructed and the tasks to be performed using the said information system, information system security officers shall seek advice from the chief information security advisor, etc. regarding the security requirements formulated according to the classification of the information system, and based on the characteristics of the tasks and the information system, check whether there is a need to include higher level information security measures as security requirements.

5.2.2 Procurement and construction of information systems

Purpose

When procuring and constructing information systems, it is necessary to procure an equipment based on the selection criteria and to carry out information system measures at the development phase of the system, in order to appropriately implement information security measures in accordance with the prescribed security requirements.

It is also required to conduct system inspections following the established/maintained inspection procedures at the time of delivery or reception of information systems, to ensure appropriate incorporation of security and management functions to protect the information handled by such systems.

Provisions in 4.1 “Subcontracting” shall be referred to and observed when subcontracting construction of information systems. Provisions in 4.2 “Use of Cloud Services” shall be referred to and observed when using a cloud service to construct information systems. Provisions in 4.3 “Procurement of Equipment, etc.” shall be observed when procuring equipment, etc. to be used in information systems.

Compliance Requirements

(1) Measures when constructing information systems

(a) When constructing information systems, information system security officers shall implement measures deemed necessary from perspectives of information security.

(b) When the constructed information systems are migrated to the operation and maintenance phase, information security officers shall implement the measures for procedures and environments of migration deemed necessary from perspectives of information security.

(c) When newly constructing or updating an information system, information system security officers shall record or write information about security requirements in the information system ledger and report it to the head information security officer.

(d) Information system security officers shall maintain documents required to implement information securities measures for the information systems under their management, containing all the information system-related documents specified below.

(i) Information of the server equipment and terminals composing the information systems

(ii) Information of the communication lines and communication equipment composing the information systems

(e) Information system security officers shall maintain documents required to implement information securities measures for the information systems under their management, containing all the operating procedures specified below.

(i) Procedures to maintain the security level of information security of each component of the information systems

(ii) Procedures when detecting information security incidents

(iii) Procedures for recovery in the event of an information system failure

(2) Measures for inspections on delivery

(a) Information system security officers shall conduct validations and inspection at the time of delivery, following the inspection procedures prescribed in the procurement specifications and so on, in order to ensure the procured equipment, etc. and the received information systems are conforming to the requirements for information security measures.

(b) When an information system transitions from the development phase to the operation and maintenance phase, information system security officers shall confirm that content necessary for information security measures is included in the items handed down from the developer of the information system in question to its operator/maintainer.

5.2.3 Operation and maintenance of information security

Purpose

When information systems are migrated to the operational phase, it is necessary to establish the resource allocation system in operation, and to perform regular checks of parameters settings on the equipment and other components, as well as to manage records of operation and maintenance, in order to ensure proper implementation of the security requirements determined upon planning, procurement, and construction of the system.

Most of information security incidents normally occur during operation, so it is important to duly monitor the operation of information systems to confirm effectiveness of the implemented information security measures.

Also, the information security measures for system maintenance need to be appropriately implemented in the same manner as those for system operation. In those cases such as individually outsourcing system maintenance work, it is essential to duly implement the information security measures in accordance with the government agency's own standards. When subcontracting the operation and/or maintenance of information systems, refer to 4.1 "Subcontracting."

Furthermore, refer to 4.2 "Use of Cloud Services" for the operation and maintenance of information systems constructed using a cloud service and 5.4 "Shared Government Systems" for the operation and maintenance of information systems constructed using a shared government system.

Compliance Requirements

(1) Measures for information systems during operation and maintenance

(a) Information system security officers shall appropriately operate the security functions, including monitoring, incorporated to the system during its operation and maintenance.

(b) Information system security officers shall manage the records of operation and maintenance, in order to facilitate tracing of incidents such as malicious activities and unintended access to the systems. Whenever there is a change in the configuration or settings of equipment due to operation or maintenance, information system security officers shall check whether the information security measures are appropriate and make revisions as necessary.

(c) When a change occurs to the content of the information system ledger and relevant document(s) regarding the operation or maintenance of an information system, information

system security officers shall update or correct the information system ledger and relevant document(s). Such update or correction in the information system ledger shall be reported to the head information security officer.

(d) Information system security officers shall perform review and revision as necessary whenever a new threat emerges or according to the situation of operation, monitoring, etc. and take necessary information security measures for the information system.

(e) Information system security officers shall operate information systems that handle confidential information in such a way that enables them to take appropriate measures in the case of a critical event.

5.2.4 Update and disposal of information systems

Purpose

When updating or disposing of information systems, it is necessary to prevent leakage of highly confidential information contained in the system during disposal or recycling.

If the highly confidential information is saved on the information systems, or classifications or handling restrictions of information stored on the systems are unclear, it is essential to implement measures to ensure complete erasure of such information.

Compliance Requirements

(1) Measures for update and disposal of information systems

(a) When updating or disposing of information systems, information security officers shall implement all of the following measures, taking into account of classifications and handling restrictions of the information stored in said systems.

(i) Information security measures for transferring data when updating information security systems.

(ii) Erasure of unnecessary data when disposing of information security systems

5.2.5 Review on measures for information systems

Purpose

As the environments surrounding information security are constantly changing, the level of information security cannot be maintained if emerging threats are not precisely addressed. For this reason, it is necessary to review information security measures by means of periodic checks, and conduct further reviews by means of ad-hoc checks in the event of drastic changes in external environments, and so on. In addition to reviews by means of periodically checking information security measures in the operation phase, it is necessary to review information security measures based on measures promotion plans and revise information security measures that necessitate improvements across Agencies based on self-checks, audit, and headquarters audit results.

Compliance Requirements

(1) Review on measures for information systems

(a) Information system security officers shall appropriately review the information security measures for information systems based on measures promotion plans.

(b) Information system security officers shall appropriately review information security measures based on instructions for improvement deriving from reviews on information security measures for which improvement is necessary across Agencies. The results of measures shall be reported to the head information security officer.

5.3 Operational Continuity Plan of Information Systems

5.3.1 Ensuring consistency between information security measures for information systems and the systems' operational continuity plans

Purpose

It is essential, even in crisis events such as earthquakes, fire, infectious diseases, and information security incidents, to ensure the continuity of business whose interruption may cause a serious threat to the safety and benefit of citizens. As such, national administrative organs establish and carry out business continuity plans for government agencies and operational continuity plans for information systems. Incorporated Administrative Agencies and Designated Corporations likewise establish and carry out corporate business continuity plans and operational continuity plans for information systems according to the characteristics of their work following their mid-term targets and other instructions. On the other hand, to continue operation of information systems at the time of a crisis event, it is vital to examine and determine the measures, as well as operational rules and operating procedures, for information security in crisis events.

It is also necessary to ensure that the requirements prescribed in such business continuity plan and information system operational continuity plan, and those prescribed in the information security related provisions are in accordance with each other, and contain no inconsistencies among them.

Compliance Requirements

(1) Ensuring consistency between information security measures for information systems and the systems' operational continuity plans

(a) To set in place information system operational continuity plans, which support the highly prioritized tasks during emergencies at Agencies, the head information security officer shall review the establishment of matters related to measures, as well as operational rules and operating procedures, for information security in crisis events.

(b) The head information security officer shall periodically confirm if the information security measures, operational rules, and operating procedures for information systems in crisis events are feasible in line with the operational continuity plan of information systems.

(c) The head information security officer shall periodically review the information security measures, operational rules, and operating procedures for information systems in crisis events according to the operational continuity plan of information systems.

5.4 Shared Government Systems

5.4.1 Measures by shared government system administrator agencies

Purpose

Shared government systems are operated through a collaboration of administrator agencies and user agencies for shared government systems. For this reason, preventive measures must be taken to ensure that there are no holes in information security measures among the Agencies. Furthermore, considering the possibility of any information security incident on some information systems using a shared government system affecting other information systems using the same shared government system, the shared government system administrator agencies must appropriately manage the information security of the entire shared government system and properly ensure a certain level of information security.

Therefore, the responsibilities and role division of the administrator and user agencies must be clarified, establishing a structure that can quickly, solidly, and collaboratively respond to any information security incident detected.

Compliance Requirements

(1) Establishment/Maintenance of operation and management rules for information security measures

(a) When constructing a shared government system, information system security officers shall establish/maintain operation and management rules for information security measures that include all of the following and build sufficient consensus with shared government system user agencies.

(i) Demarcation of responsibilities between shared government system administrator agencies and user agencies

(ii) Cooperation/Collaboration structure for normal times and emergencies

(iii) Specific action plans for emergencies

(2) Establishment/Maintenance of information system ledger and documents related to information systems

(a) The head information security officer of shared government system administrator agencies shall establish/maintain the information system ledger for shared government systems established as per Compliance Requirements 2.1.2(1)(a), containing matters regarding security requirements for shared government system user agencies.

(b) Information system security officers of shared government system administrator agencies shall establish/maintain the documents related to information systems for shared government systems established as per Compliance Requirements 5.2.2(1)(d), containing information related to shared government system user agencies.

5.4.2 Measures by shared government system user agencies

Purpose

Shared government system user agencies must properly use shared government systems in line with the defined responsibilities and role division while ensuring the required structure based on the operation and management rules set forth by shared government system administrator agencies. Furthermore, due to the need for both administrator agencies and user agencies to cooperate with each other in dealing with detected information security incidents, it is important to clarify, based on the operation and management rules set forth by the administrator agencies, the responsibilities and role division that apply to the agencies in the event of an information security incident while also sharing among the agencies the information necessary for taking measures.

Compliance Requirements

(1) Establishment/Maintenance of framework at shared government system user agencies

(a) When constructing an information system using the security functions provided by a shared government system, information system security officers shall request that the chief information security officer ensures the framework in accordance with the operation and management rules set forth by the shared government system administrator agencies.

(b) When receiving a provision of equipment, etc. provided by the shared government system for use by employees of the Agency, the head information security officer shall assign a shared government system user administrator for each shared government system as a manager that manages the tasks concerning the information security measures for that use.

(c) For using the shared government system, the shared government system user administrator shall request that the chief information security officer ensures the framework in accordance with the operation and management rules set forth by the shared government system administrator agency.

(2) Information security measures by shared government system user agencies

(a) When constructing an information system using the security functions provided by a shared government system, information system security officers shall properly formulate security requirements so as to operate the information system in such a way that maintains the information security level of the shared government system, based on the operation and management rules set forth by the shared government system administrator agencies.

(b) Information system security officers shall, based on the operation and management rules set forth by the shared government system administrator agencies, appropriately deal with information security incidents regarding shared government systems.

(3) Management of equipment, etc. of shared government system user agencies

(a) When receiving a provision of equipment, etc. provided by the shared government system for use by employees of the Agency, the shared government system user administrator shall formulate operational rules and operating procedures for the information security measures

for using the shared government system.

(b) The shared government system user administrator shall establish documents necessary for understanding the provided equipment, etc. for the shared government system.

(c) The shared government system user administrator shall provide the shared government system administrator agencies with the information they need to organize the information system ledger and the documents related to information systems and also promptly report any changes to such information.

(d) The shared government system user administrator shall, based on the operation and management rules set forth by the shared government system administrator agencies, appropriately deal with information security incidents on shared government systems.

Chapter 6 Information Systems Components

6.1 Terminals

6.1.1 Terminals

Purpose

When using terminals, caution must be used for leakage of stored information due to external causes, such as malware infection and intrusions. Moreover, internal causes such as improper system handling or negligence of employees might result in information security incidents, including malware infection. Taking these risks into account, it is important that proper security measures be taken for terminals used by employees while also defining which software can be used and which equipment, etc. can be connected to the terminals. As for the mobile use of physical terminals, there is a higher risk of information leakage caused by theft or loss and so on, of the device. These issues should be taken into consideration when implementing measures.

In addition to the requirements in this provision, requirements regarding measures for functions such as user/entity authentication, access control, authority control, and log management in section 7.1 “Security Functions for Information Systems”, section 7.2.1 “Measures against software vulnerabilities”, section 7.2.2 “Measures for protection against malware”, and section 6.4.4 “IPv6 communication lines” should also be complied with.

Compliance Requirements

(1) Measures when introducing terminals

(a) For physical terminals which handle classified information, information system security officers shall implement measures against physical threats such as theft and unauthorized removal of terminals, unauthorized use of terminals by malicious third parties, as well as unauthorized viewing of display devices of terminals.

(b) To eliminate the possible increase in vulnerability due to use of variety of software, information system security officers shall specify the software of which use is approved and prohibit the use of any other software.

(c) Information system security officers shall define equipment, etc. that can be connected to the terminals and prohibit the connection of any other equipment, etc.

(d) Information system security officers shall, according to the security requirements for the information system, implement proper security measures for the terminals.

(e) Information system security officers shall implement measures against known vulnerabilities in software approved for use on the terminals.

(2) Measures when operating the terminals

(a) Information system security officers shall, by means of periodic checks, conduct a review of software which is approved to be used on the terminals.

(b) Information system security officers shall periodically verify the status of all software used on the terminals under their management, and implement corrective measures when identifying any terminal in inappropriate status, and so on.

(3) Measures when terminating the operation of terminals

(a) Information system security officers shall erase all the information stored on the external storage media of the terminal when terminating its operation.

6.1.2 Measures when using terminals outside areas requiring control measures

Purpose

Due to the acceptance of teleworking, an increasing number of employees are working outside of Agencies. When they work outside of areas requiring control measures, using physical terminals furnished by Agencies, it increases the risk of snooping, theft and loss. In order to address such risks, it is necessary to establish procedures for use and permission for use, and to ensure that employees comply with these procedures when they use physical terminals furnished by Agencies outside areas requiring control measures. It is also necessary to take technical measures to prevent information from being stolen through theft or loss of terminals or infection of terminals with malware.

Furthermore, when employees remotely access information systems using external communication lines, it is necessary to implement security measures to combat remote access-specific attacks, etc. For more information on remote access, refer to Compliance Requirements 8.1.3(2).

When constructing a remote access environment on an information system using external communication lines, it is effective to implement dynamic access control, which is part of a function that realizes a mechanism that continuously authenticates and approves the status of entities, etc. for every access request. Not only the first access request to access an information system is controlled, but each access request is examined for trustworthiness; if any access request is deemed not to be trustworthy, an addition measure is implemented. For more information on dynamic access control, refer to 7.3 “Zero Trust Architecture.”

Compliance Requirements

(1) Establishment/Maintenance of operational rules for the adoption and use of Agency-furnished terminals (only when used outside of areas requiring control measures)

(a) In preparation for cases where employees handle classified information through the use of Agency-furnished physical terminals (only when used outside of areas requiring control measures), head information security officers shall establish usage protocols and approval procedures as operating procedures, taking into account the risks of information leakage from these terminals and the communication lines used.

(b) Head information security officers shall establish operational rules related to technical measures to prevent the theft of data as a result of theft, loss, infection with malware, etc. for Agency-furnished physical terminals (only when used outside of areas requiring control measures) that handle confidential information.

(c) In cases where approval is granted to connect Agency-furnished physical terminals connected to communication lines outside the Agency outside of areas requiring control measures to communication lines inside the Agency after whether or not to approve this has

been reviewed and a decision to approve has been made, the head information security officers shall establish operational rules related to technical measures that take into account the risk of information systems being infected with malware from said terminals via communication lines inside the Agency.

(2) Measures for the adoption and use of Agency-furnished terminals (only when used outside of areas requiring control measures)
   (a) When employees use Agency-furnished physical terminals (only when used outside of areas requiring control measures) for handling confidential information, information system security officers shall take technical measures for such terminals as specified in (b) in the preceding article.
   (b) When having Agency-furnished physical terminals connected to external communication lines outside of areas requiring control measures connect to internal communication lines, information system security officers shall take technical measures for such terminals as specified in (c) in the preceding article.

6.1.3 Measures for the adoption and use of non-Agency-furnished terminals

Purpose

Agency's tasks should be performed by using the terminals furnished by the Agency. Nevertheless, there may be cases of crisis events (or business trips or being out of office) where information processing has to be performed using terminals that are not furnished by the Agency. In such cases, the information security level of such terminals may not satisfy the government agency's own standards. Therefore, if a non-Agency-furnished terminal may be used for tasks, it is necessary to properly evaluate whether that terminal ensures the information security level required for use, and upon restricting available functions and implementing additional security measures to make it usable for tasks, have employees use the terminal under strict control of the Agency.

Non-Agency-furnished terminals are managed by the owner of the terminal. Whether it can be used for tasks needs to be determined based on the consideration of risks associated with it not being under the control of the Agency. Even when the use of such non-Agency-furnished terminals is approved, it is still necessary to establish a use permission procedure and have the users comply with the established provisions and procedures for handling information.

Compliance Requirements

(1) Decision on the usability of non-Agency-furnished terminals
   (a) The chief information security officer shall determine the advisability of using non-Agency-furnished terminals at the Agency by taking into consideration the prospects for meeting the required information security standards when doing so. This determination shall also be based on factors such as the classification of the information to be handled and restrictions on handling it, the security control measures taken by the Agency, and the understanding that the management of the terminal in question is carried out by its owner instead of the

Agency.

(2) Establishment/Maintenance of operational rules for the use of non-Agency-furnished terminals

(a) The head information security officer shall establish procedures for granting approval and so on as operating procedures when employees perform information processing pertaining to the Agency's work through the use of non-Agency-furnished terminals.

(b) In preparation for cases where employees handle classified information through the use of non-Agency-furnished terminals, the head information security officer shall establish usage protocols and approval procedures as operating procedures, taking into account the risks of information being taken due to theft, loss, or infection with malware.

(c) The head information security officer shall establish the operational rules related to security control measures, including technical measures for preventing information from being taken due to theft, loss, or infection with malware for non-Agency-furnished terminals that handle confidential information.

(d) In cases where approval is granted to connect non-Agency-furnished terminals connected to communication lines outside the Agency outside of areas requiring control measures to communication lines inside the Agency after whether or not to approve this has been reviewed and a decision to approve has been made, the head information security officer shall establish operational rules related to security control measures and operating procedures related to approval procedures that take into account the risk of information systems being infected with malware from said terminals via communication lines inside the Agency.

(3) Designation of officers responsible for the use of non-Agency-furnished terminals

(a) Information security officers shall designate officers responsible for managing the implementation status of security control measures concerned with processing the information involved in the Agency's operations through the use of non-Agency-furnished terminals (hereinafter referred to as "terminal management officers").

(4) Measures for using non-Agency-furnished terminals

(a) Employees shall acquire permission from a terminal management officer when performing information processing for the Agency's tasks using a non-Agency-furnished terminal.

(b) Employees shall observe the use procedures specified in (2)(b) when handling confidential information using a non-Agency-furnished terminal.

(c) Terminal management officers shall take the security control measures specified in (2)(c), or have employees take such measures, for the non-Agency-furnished terminals handling confidential information.

(d) Upon completion of the purpose of information processing, employees shall delete the confidential information from the non-Agency-furnished terminals.

6.2 Server Equipment

6.2.1 Server equipment

Purpose

Server equipment such as e-mail servers, webservers, and file servers normally store large size of information, so that the impact of leakage and manipulation of such information is far larger than that of terminals. In addition, server equipment is subject to a higher risks of malware infection and intrusions, because their functions are generally utilized via communication lines. If the server equipment used by Agencies were used for unauthorized access or relaying spam e-mails, it would seriously undermine the public trust in these Agencies.

Moreover, as a large number of users simultaneously use server equipment, failure of its functions would result in a greater impact. These issues should be taken into consideration when implementing measures.

In addition to the requirements in this provision, requirements regarding measures for functions such as user/entity authentication, access control, authority control, log management, and measures for monitoring function and other functions set forth in section 7.1 “Security Functions for Information Systems”, as well as requirements concerning server equipment set forth in section 7.2.1 “Measures against software vulnerabilities”, section 7.2.2 “Measures for protection against malware”, section 7.2.3 “Measures against denial-of-service attacks”, and section 6.4.4 “IPv6 communication lines” should be complied with. For the maintenance of server equipment conducted via an external communication line, the measures for remote maintenance as set forth in 6.4.1 “Communication lines” should be implemented. For e-mail servers, webservers, DNS servers, and database in particular, the requirements set forth in this section should be complied with, in addition to the common measures stipulated in this provision.

Compliance Requirements

(1) Measures when implementing server equipment

(a) For physical server equipment which handles classified information, information system security officers shall implement measures against physical threats such as theft and unauthorized removal of server equipment, unauthorized use of server equipment, as well as unauthorized viewing of display devices of server equipment.

(b) To prevent situations where services are suspended due to failure, excessive access, and other problems with information systems which handle vital information, information system security officers shall ensure system’s availability by setting up the server equipment for such services in a redundant configuration, and so on.

(c) To eliminate the possible increase in vulnerability due to use of variety of software, information system security officers shall specify the software which is approved to be used on the server equipment and prohibit the use of any other software.

(d) Information system security officers shall specify equipment, etc. that can be connected to server equipment and prohibit the connection of any other equipment, etc. to the server equipment.

(e) Information system security officers shall, according to security requirements for information systems, implement proper security measures on server equipment.
(f) Information system security officers shall implement measures for known vulnerabilities in software used on server equipment.
(g) Information system security officers shall create a server equipment backup using proper methods, for server equipment that handles vital information.

(2) Measures when operating the server equipment
(a) Information system security officers shall, by means of periodic checks, conduct a review of software which is approved to be used on the server equipment.
(b) Information system security officers shall periodically verify the software and configuration of all server equipment under their management, and implement corrective measures when identifying any server equipment in inappropriate status, and so on.
(c) Information system security officers shall implement measures to monitor the server equipment for the purpose of monitoring the server equipment for information security incidents.
(d) Information system security officers shall operate server equipment that handles vital information in such a way that enables appropriate action in the event of a crisis event.

(3) Measures when terminating the operation of server equipment
(a) Information system security officers shall delete all information stored on the external storage media of server equipment when terminating its operation.

6.2.2 E-mail

Purpose

As sending and receiving e-mails is nothing but an exchange of information, there are risks against confidentiality, including information leakage caused by inappropriate use, as well as risks that employees who use e-mail to be victimized by illegal acts abusing e-mails, such as impersonation by malicious third parties. In order to prevent these problems, proper e-mail server management is essential.
In addition to the requirements in this provision, the same for the server equipment in section 6.2.1 “Server equipment” should be complied with.

Requirements

(1) Measures when introducing e-mail services
(a) Information system security officers shall set up the e-mail servers, ensuring no illegal e-mail relaying occurs.
(b) Information system security officers shall provide functions of user/entity authentication when sending and receiving e-mails between e-mail clients and servers.
(c) Information system security officers shall implement measures to prevent e-mail spoofing.

(d) Information security officers shall take measures to encrypt communications between e-mail servers in order to prevent the theft or manipulation of e-mails sent over the internet.

6.2.3 Web

Purpose

Webservers are open to public access on the internet and under constant risk of attacks. As possible damage includes manipulation of web contents (information published on web pages), webservers to be made unavailable, and inducement to false website, it is necessary to address such damage by combining appropriate measures and implement them.

In addition to requirements in this section, the same for the server equipment in section 6.2.1 "Server equipment" should be complied with. For web applications on web servers, refer to 6.6 "Applications and Content."

Compliance Requirements

(1) Measures when introducing and operating webservers

(a) In order to prevent increased possibility of vulnerabilities, information system security officers shall only use the necessary functions out of all the web server functions.

(b) Information system security officers shall take measures to prevent unintended information leaks from web servers.

(c) Information system security officers shall restrict entities who edit web contents.

(d) Information system security officers shall take measures such as encryption of all information and certification using electronic certificates for the purpose of preventing theft and tampering of information transferred over the Internet.

6.2.4 Domain Name Systems

Purpose

A domain name system (DNS: Domain Name System) is hierarchical and decentralized system on the internet which is mainly used to manage correspondence (forward lookup and reverse lookup) between host names on the internet or domain names in E-mail and IP addresses. DNS serves, after receiving queries from clients (DNS clients) including terminals to return responses such as corresponding relationships between IP addresses and domain names and host names. DNS includes content servers which return responses to queries about the domains which the government agency manages and cache servers which make queries to content servers according to queries from DNS clients. If a cache server becomes unavailable, the websites and e-mails which use the host names and the domain names, etc. will be unusable. In addition, if the integrity of information supplied by a content server is compromised and incorrect information is provided, there is a risk of damage such as DNS clients, including terminals, will be connected to malicious servers. Furthermore, if there is any error in the setting of a DNS, detection of e-mail spoofing becomes impossible, because the DNS partially handles the measure against spoofing of e-mails. To avoid such problems, appropriate DNS server management is essential.

In addition to the requirements in this provision, the same for server equipment in section 6.2.1 “Server equipment” should be complied with (excluding cases where SaaS cloud services are used).

Compliance Requirements

(1) Measures when introducing the DNS
   (a) For the content servers which provide name resolution to information systems handling vital information, information system security officers shall implement measures to ensure there is no interruption to the name resolution.
   (b) For the cache servers, information system security officers shall implement measures to ensure appropriate responses to the name resolution queries.
   (c) When the content servers are used to provide the resolution of the names exclusive to their own government agency, information system security officers shall implement measures to ensure no such information managed in said content server is leaked outside of the Agencies.

(2) Measures when operating the DNS
   (a) When installing multiple DNS content servers, information system security officers shall maintain consistency among the servers with regards to the information of the domains under their management.
   (b) Information system security officers shall periodically verify the accuracy of the information about the domains managed on the DNS content servers.
   (c) Information system security officers shall take measures to maintain appropriate responses to name resolution requests on cache servers.

6.2.5 Database

Purpose

“Database” described in this provision means server equipment composed of database management system and the data files, which storages classified information, which manages the data constructed systematically and has several functions which can easily serve for searching, extracting and so forth. There are various risks for database which storages classified information, for example, the risk by external factors such as malware infection or the unauthorized access and the risk by the internal factors such as the inappropriate use or negligence by employees. It is necessary to take technical measures to prevent an abuse of the administrator authority.

Especially, a database storing a large quantity of data may will be a target of cyber-attacks. Breach of such a database has considerable impact on administrative affairs.

In addition to the requirements in this provision, requirements regarding measures for functions such as user/entity authentication, access control, log management, and encryptions and digital signatures in section 7.1 “Security Functions for Information Systems”, section 7.2.1 “Measures against software vulnerabilities”, section 7.2.2 “Measures for protection against malware”, and section 6.4.4 “IPv6 communication lines” should also be complied with.

Compliance Requirements

(1) Measures when implementing or operating the database

(a) Information system security officers shall appropriately perform authority control of administrator's privileges to prevent malicious operations which are internally performed.

(b) Information system security officers shall implement appropriate measures to specify the users who access data stored in database.

(c) Information system security officers shall implement measures to detect malicious operations which are performed by a user having authority to access internal data.

(d) Information system security officers shall implement measures to prevent malicious operations of data, which abuses the vulnerabilities of database or equipment, etc.

(e) Information system security officers shall appropriately encrypt the data which have to be prevented from leaking caused by malicious method or theft of electric and magnetic storage media.

6.3 Multifunction devices and equipment for specific purposes

6.3.1 Multifunction devices and equipment for specific purposes

Purpose

Multifunction devices, containing a combination of printer, fax, image scanner, and copier functions, are used at Agencies. These multifunction devices are often connected to internal communication lines, as well as to the public telephone networks and other communication lines when in use, in which case various kinds of threats are expected, because many services including web console, file transfer, file sharing, as well as remote maintenance will be operating on such devices.

Moreover, information systems for specific purposes, such as systems for video conference, IP phone, network camera, entry control systems, facility management systems, and environment monitoring systems are also used at Agencies. In many cases, equipment for specific purposes is equipped with Internet connectivity, which are commonly called IoT devices. Examples include, among the components of a network camera system, cameras that have Internet connectivity, and among the components of an environment monitoring system, sensors that have Internet connectivity. Numerous attacks that exploit vulnerabilities in these IoT devices have occurred in recent years, and attacks such as those in which IoT devices are used as a jumping-off point to attack other information systems have come to pose a social problem. Therefore, information security measures must be taken for these devices as well.

Given these situations, it is important to treat these multifunction devices and equipment for specific purposes, including IoT devices, as part of the information system components, and to implement measures in an appropriate manner by assigning personnel and clarifying who is in charge.

Compliance Requirements

(1) Multifunction devices

(a) When procuring multifunction devices, information system security officers shall establish appropriate security requirements according to functions, installation environments, as well as classification and handling restrictions of information handled by such devices.

(b) Information system security officers shall implement measures for information security incidents against multifunction devices while in operation, by taking actions such as to appropriately set up the functions available on said devices.

(c) Information system security officers shall delete all information stored on the external storage media of multifunction device when terminating its operation.

(2) Equipment for specific purposes, including IoT devices

(a) For equipment for specific purposes, if there are possible threats depending on information handled, methods of use, and connection types of the communication lines and so on, information system security officers shall implement measures suitable for the characteristics of said equipment

6.4 Communication Lines

6.4.1 Communication lines

Purpose

Most of unauthorized access and denial-of-service attacks against server equipment and terminals are carried out through the communication lines and the communication line equipment. Therefore, when implementing information security measures for communication lines and communications line equipment, it is necessary to examine potential risks thoroughly and implement measures at the constructing phase of information systems. Types of information security risks vary depending on the communication line providers and the physical line types. These differences should be fully taken into account when implementing measures.

In addition, configuration of the communication lines and conditions of information systems connected to them at the launch of information systems may change after operating them for a certain period of time. Also, there may be some changes in types of attacks.

The measures estimated to be sufficient at the construction phase of information systems may become insufficient, so it is vital to continually implement measures throughout the operation of communication lines.

Compliance Requirements

(1) Measures when installing communication lines

(a) During the communication lines installation, information system security officers shall select appropriate line types according to the classification and handling restrictions of the information handled by the information systems connected to the communication lines, and implement measures necessary for said lines to prevent impacts of information security

incidents.

(b) Information system security officers shall have the communication lines equipped with the functions to perform access control and route control on the server equipment and terminals.

(c) Information system security officers shall implement measures to ensure the confidentiality of communication contents, if assuring the confidentiality thereof is deemed necessary when connecting information systems handling confidential information to the communication lines.

(d) Information system security officers shall implement measures, which enable them to confirm that the information system is the one that employees are approved to be connected to the communication lines. The same shall apply when connecting non-Agency-furnished terminals to communication lines inside the Agencies.

(e) Information system security officers shall implement measures to ensure continuous operation of communication lines connected to the information systems handling vital information.

(2) Measures when connecting to non-Agency communication lines

(a) When connecting the internal communication lines to the external communication lines such as internet access lines and public communication lines, information system security officers shall implement measures to ensure the information security of the internal communication lines and the information systems connected to them.

(b) Information system security officers shall implement measures to monitor malicious transmissions between the internal communication lines and the external communication lines, as well as within internal communication lines.

(c) Information system security officers shall ensure information security of remote maintenance conducted on equipment, etc. connecting to internal communication lines from external communication lines for maintenance and diagnostic purposes.

(d) When using communication line services of telecommunication carriers, information system security officers shall establish agreements, upon signing a contract with the subcontractors who construct information systems, on measures to ensure the level of information security of said line services as well as its service level.

(3) Measures when operating communication lines

(a) Information system security officers shall appropriately perform route control and access control, and review and revise its settings when any change made to the communication lines and the requirements for establishing communication. This review shall also be conducted periodically.

(b) Information system security officers shall conduct reviews by means of periodic checks of monitoring targets and methods for monitoring malicious transmissions between internal communication lines and external communication lines, as well as within internal communication lines.

(c) Information system security officers shall conduct reviews by means of periodic checks of

information security measures on remote maintenance conducted on equipment, etc. connecting to internal communication lines from external communication lines for maintenance and diagnostic purposes.

(d) In the event of incidents which endanger information security of certain information system, information security officers shall protect other information systems which share the communication lines with the endangered information system, by changing the line configuration to establish a closed and independent communication line, separated from the shared ones.

6.4.2 Communication line equipment

Purpose

Communication line equipment that can be accessed from external networks such as the Internet may fall target to unauthorized access taking advantage of software vulnerabilities. For this reason, measures for software vulnerabilities should be swiftly and properly implemented in communication line equipment. Since communication line equipment is used in route control and access control for terminals and server equipment, necessary security measures must be implemented upon fully considering the risks from the construction phase of the information system. It is also important to continuously implement measures during the operation phase as well, in response to changes in the trend of threats.

Compliance Requirements

(1) Measures when introducing communication line equipment

(a) When installing physical communication line equipment, information system security officers shall ensure that destruction and unauthorized operation by a third party are not possible.

(b) Information system security officers shall establish operating procedures including matters related to software necessary for operating communication line equipment.

(c) Information system security officers shall, according to the requirements for information system network configuration defined as security requirements for information system, implement proper security measures for communication line equipment.

(d) Information system security officers shall take measures for known vulnerabilities in software used on communication line equipment.

(2) Measures when operating communication line equipment

(a) When changing settings of communication line equipment in relation to operation or maintenance of the communication line equipment, information system security officers shall keep a record of the work in case of an investigation into any information security incidents.

(b) For communication line equipment that is part of an information system that handles vital information, information system security officers shall keep a backup of settings necessary

for recovering operational state.

(c) Information system security officers shall inspect the state of software necessary for the operation of communication line equipment and take measures for any vulnerabilities found.

(3) Measures when terminating the operation of communication line equipment

(a) When terminating the operation of communication line equipment, information security officer shall take appropriate measures, such as erasing all the information recorded on the external storage media on said equipment to prevent leakage of information stored during the operation, in case that such equipment composing the communication lines are reused or discarded after terminating its operation.

6.4.3 Wireless LAN

Purpose

Wireless LAN needs protective measures against threats deriving from the ease of interception of communications compared to wired networks since it uses radio waves, in addition to threats anticipated in wired networks and communication line equipment.

Aside from the Compliance Requirements below, the compliance requirements for measures to be taken upon introduction set forth in 6.4.1 “Communication lines” and 6.4.2 “Communication line equipment” must also be complied with.

Compliance Requirements

(1) Measures when introducing wireless LAN environments

(a) When constructing the internal communication lines with wireless LAN technologies, information system security officers shall, on top of implementing the common measures for communication line construction, encrypt the communication routes to ensure the confidentiality of communication contents, then implement other measures required to ensure information security.

6.4.4 IPv6 communication lines

Purpose

In recent years, a large number of server equipment, terminal, and communication line equipment, etc. which are equipped with IPv6 communication technology (hereinafter referred to as “IPv6 communications”) by default have been released. With the IPv6 communication protocol, direct packet routing using global IP addresses must be considered, as unintended IPv6 communications could occur on the communication network due to inadequate settings, which may be abused for unauthorized access. Therefore, necessary measures should be implemented.

Compliance Requirements

(1) Measures related to information systems with IPv6 communications

(a) When constructing information systems using IPv6 technologies for communication,

information system security officers shall select, when possible, a Phase-2 compliant product based on the IPv6 Ready Logo Program, as the equipment, etc. to procure.

(b) For information systems to be constructed are expected to perform communication with IPv6 technology, information system security officers shall take into account the characteristics of IPv6 communication and so on, and review the threats and vulnerabilities for information security deriving from IPv6 communication, and shall implement necessary measures.

(2) Control and monitor for unintended IPv6 communications

(a) When connecting server equipment, terminals and communications line equipment to communication lines for which no IPv6 communication is intended, the information system security officers shall implement measures to control IPv6 communications in order to prevent information security threats caused by unauthorized IPv6 communications received from said lines, such as arrival of unexpected IPv6 communication packets as a result of automatic tunneling functions.

6.5 Software

6.5.1 Software that manages or controls information system platforms

Purpose

Software that manages or controls information system platforms is equipped with important security functions for controlling information systems. When such software is abused or accessed without due authority, damage may be extensive. For this reason, necessary security measures must be implemented in terminals and the software itself, as well as on server equipment and communication line equipment that uses software that manages or controls information system platforms.

This section describes particularly necessary security measures when using software that manages or controls information system platforms from the measures required in 7.1 “Security Functions of Information Systems.” Aside from this section, requirements described in the introduction of user/entity authentication function specified in 7.1.1 “User/Entity authentication function,” the introduction of access control function specified in 7.1.2 “Access control function,” the control of authority specified in 7.1.3 “Authority control,” and the acquisition of logs specified in 7.1.4 “System logs retrieval and management” must also be met. It is important to take appropriate measures based on the function and specifications of the software that manages or controls information system platforms.

In order to prevent mistakes in operation and setup when using such software, it is also important to establish procedures that enable software users and administrators to use the software. Furthermore, measures for software vulnerabilities are particularly important for preventing attacks made by abusing the software that manages or controls information system platforms. It is necessary to review measures that shorten the time for the application of security patches as much as possible according to the degree or impact and urgency of the unknown vulnerabilities, while also enabling notifications

of information on vulnerabilities in the software from the product vendor or vulnerability information provision sites. It is important to take solid measures for vulnerabilities by referring to 7.2.1 “Measures against software vulnerabilities.”

Compliance Requirements

(1) Measures when introducing software that manages or controls information system platforms
   (a) Information system security officers shall take measures to protect, from an information security perspective, the software itself, as well as the terminals, server equipment, and communication line equipment on which the software that manages or controls information system platforms is installed.
   (b) Based on the characteristics of the software used, information system security officers shall establish/maintain all of the following operating procedures.
      (i) Procedures for maintaining the information security standards for the software that manages or controls information system platforms
      (ii) Procedures for handling information security incidents detected in the software that manages or controls information system platforms

(2) Measures when operating software that manages or controls information system platforms
   (a) When operating or maintaining software that manages or controls information system platforms, information system security officers shall implement all of the following security measures.
      (i) Measures for maintaining the security of software that manages or controls information system platforms
      (ii) Measures for swiftly detecting and responding to threats and information security incidents

6.6 Applications and Content

6.6.1 Measures upon creating and operating applications and content

Purpose

Agencies prepare applications and contents and make them widely available to offer administrative services such as providing information, executing administrative procedural tasks, and collecting opinions. The information security level of user's terminal should not be deteriorated when using these applications and contents. Agencies need to implement information security measures when providing applications and contents. In addition, when subcontracting the development and provisions of applications and contents, the requirements in section 4.1 "Subcontracting" should be observed.

Compliance Requirements

(1) Establishment/maintenance of operational rules related to creation of applications and contents
   (a) The head information security officer should maintain the operational rules to prevent actions which cause deterioration of information security level of the systems other than those of their own Agencies when providing applications and contents.

(2) Formulation of security requirements for applications and contents
   (a) Information security officer shall establish security requirements for applications and content and include them in the specifications in order to prevent deterioration of the level of information security of the users other than those of their own Agencies.
   (b) When subcontracting the development and creation of applications and contents, employees shall include the requirements as per the preceding paragraph.

(3) Measures for developing applications and content
   (a) In the development of web applications, information system security officers shall take measures to eliminate known vulnerabilities in web applications in addition to implementing the specifications defined as security requirements.

(4) Measures for operating applications and content
   (a) Information system security officers shall review the methods of providing applications and web content in such a way that does not deteriorate the users' information security level.
   (b) Information system security officers shall periodically check the status of measures for vulnerabilities in the applications and content operated and take necessary measures for any vulnerabilities discovered.
   (c) Information system security officers shall take measures to detect any alterations to web applications and web content.

6.6.2 Measures upon providing applications and contents

Purpose

Agencies prepare websites and make them available to citizens to offer administrative services such as providing information, executing administrative procedural tasks, and collecting opinions. As these services provided to citizens (including cloud services) are normally used via the internet, it is important for citizens to be sure that these services are genuinely offered by authentic Agencies. Furthermore, if no measures are taken against websites which impersonate Agencies, there would be a fear that the public trust for them would be undermined, and also that the citizens could be directed to unauthorized websites, and infected with malware. Therefore, it is essential to implement measures to respond to such situations.

Compliance Requirements

(1) Use of government domain name

(a) Information system security officers shall use government domain name in the information systems, unless the government domain name cannot be acquired, so that the users can confirm that the websites offered to users outside the Agency are provided by the actual Agency itself.

(b) When subcontracting the creation of a website for users outside the Agency, the use of domain names applicable to the Agencies in question shall be specified in the procurement specifications.

(2) Prevention of users from being lured to malicious websites

(a) Information system security officers shall implement measures to prevent users from being lured, through pages such as search engine sites, to malicious websites which impersonate Agencies.

(3) Notification of applications and contents

(a) When notifying users of applications and contents, employees shall implement the measures in order to ensure that general users are led to use said applications and contents.

(b) When notifying users of applications and contents provided by the parties other than their own Agencies, employees shall keep the effectivity of URL and so on in notification.

Chapter 7 Security Requirements for Information Systems

7.1 Security Functions of Information Systems

7.1.1 User/Entity authentication functions

Purpose

In order to limit users/entities accessible to the information or the information systems, it is necessary to introduce user/entity authentication functions. It is important to take measures to prevent unauthorized access through abusing vulnerability or impersonation.

In case of providing services for general public from information systems of Agencies, it is necessary to appropriately protect user/entity authentication information, considering that it is general public who access its information systems.

Compliance Requirements

(1) Implementation of the user/entity authentication functions

(a) Information system security officers shall implement the user/entity identification and authentication functions when identification and verification of authorized users/entities are necessary.

(b) When establishing information systems that provide online procedures for submitting applications and notifications between the public or companies and Agencies, information system security officers shall formulate requirements for user/entity authentication based on an assessment of the risks involved with these online procedures.

(c) Information system security officers shall implement measures to prevent malicious activities caused by leakage of user/entity authentication information and so on, as well as the measures against unauthorized attempts of user/entity authentication.

(2) Management of the identification code and the user/entity authentication information

(a) Information system security officers shall implement measures to appropriately give identification code and user/entity authentication information to all the entities who access information systems, and manage them.

(b) Information system security officers shall implement measures to prevent malicious use of identification code and user/entity authentication information, soon after it becomes no longer necessary for the entity to use the information system.

7.1.2 Access control functions

Purpose

Access control means control of entities who access information systems and information. In case that multiple users operate information systems, risks of information leakage, etc. can be diminished by restricting access to some specific information in the information system only to entities necessary to use it.

Compliance Requirements

(1) Implementation of access control functions

(a) Information system security officers shall implement a function which enables only the authorized persons to set access control according to the characteristics of information systems, and the classification and handling restrictions of information handled in the systems.

(b) Information system security officers shall appropriately operate access control functions so as to surely restrict the entities who permit the access to information systems and information.

7.1.3 Authority control

Purpose

In order to operate appropriately access control functions of information systems, it is necessary to set appropriately authority of access from entities to the object. In doing so, the access rights granted should be limited to the minimum necessary. With no access granted by default, in principle, it is important that only the entities who need access are granted access rights, and those who do not need access are not granted access rights. Likewise, when assigning permission to information, in principle, it is important that only the entities who need to know are granted access rights, and those who do not need to know are not granted access rights. Without appropriate authority control, the risks of unauthorized access to information or information systems would arise.

Administrator authority is one of the authority control functions on the information system, which generally includes privileges to allow all operations on the system.

If such privileges were stolen by malicious third parties, there would be dangers such as leakage or manipulation of not only user/entity authentication information, but also information accessible by privileged authority, in addition to possible impact on business continuity caused by malware intended to destroy information systems and/or information. Furthermore, disabling of information security functions by unauthorized changes to settings that detect or prevent such unauthorized access and malware is a concern, and therefore, it is vital to limit the administrator authority only to the relevant users.

Compliance Requirements

(1) Authority control

(a) Information system security officers shall implement measures to set appropriately authority of access from entities to the object to the minimum necessary extent.

(b) Information system security officers shall implement measures to minimize damages caused by thefts of identification codes and user/entity authentication information of administrator’s privileges, and to prevent malicious and erroneous operations which are internally performed.

(c) Information system security officers shall periodically check for any unnecessary access rights granted for access from entities to the object.

7.1.4 System logs retrieval and management

Purpose

Logs of the information system are the records of operation, user access history, communication history, and other essential information of management of the system, which are important tools for detecting information security incidents and signs of an incident, such as unauthorized access and operations by malicious third parties.

If any incident concerning information security on the system takes place, these logs will serve as important material for identifying and clarifying the causes in the course of investigations after the incident. For this reason, information systems' logs should be duly retrieved in accordance with system specifications and need to be appropriately maintained and protected to prevent these logs from being manipulated or lost.

Compliance Requirements

(1) Event logs retrieval and management

(a) Information system security officers shall retrieve logs of information system which are necessary to verify the information systems are appropriately used and free from unauthorized access and operation.

(b) After determining the purpose to retrieve logs according to the characteristics, information system security officers shall determine items such as equipment, etc. in which logs should be retrieved, types of information recorded in the log, storage periods, as well as log information handling methods from a viewpoint of classified information handling, and appropriately manage the logs.

(c) Information system security officers shall establish a function to examine or analyze the logs retrieved from the information systems, and perform examinations or analysis to detect unauthorized access and operations, etc. by malicious third parties, and so on.

7.1.5 Encryption and digital signatures

Purpose

Encryption and digital signatures are effective means to prevent leakage and manipulation of information handled by information system, so it is essential to appropriately implement these functions to the system.

When introducing encryption and digital signatures, it is necessary to take into account the issues such as adequacy of algorithms and key length, as well as the protocols using it, measures in case that said algorithm or key length was compromised during operation or in case that a vulnerability is found in said protocol, as well as appropriate key information management.

Compliance Requirements

(1) Implementation of encryption and digital signature functions

(a) Information system security officers shall take all of the following measures to prevent leakage and manipulation of information handled by information systems

(i) Examine the necessity of encryption functions for the information systems handling confidential information, and duly implement them when it is deemed necessary.

(ii) Examine the necessity of digital signature and verification functions for the information systems handling critical information, and implement them when it is deemed necessary.

(b) Information system security officers shall, based on the "e-Government Recommended Ciphers List" whose security and performance is confirmed by CRYPTREC (the Cryptography Research and Evaluation Committees), establish encryption and digital signature algorithm and key length used on information systems, a safe protocol using them, and operating procedures for methods to operate them.

(c) When assigning a digital signature, information system security officers shall ensure the use of an appropriate public key infrastructure according to the purpose, if the one which is applicable and serves the purpose of digital signature exists, after examining the algorithm, key length, and operational methods of encryption and digital signature applied at their own Agencies.

(2) Management of encryption and digital signature

(a) Information system security officers shall take all of the following measures to ensure proper use of encryption and digital signature

(i) For the information systems which assign digital signatures, securely provide the verifiers of signatures with information and methods of verifying the validity of the signatures

(ii) For the information systems which perform encryption, or those which perform assignment or verification of digital signatures, regularly obtain information on threats which compromise the algorithm or key length selected for such operations or raise vulnerability in protocol, and share it with employees as necessary.

7.1.6 Monitoring function

Purpose

In order to verify quick detection of information security incidents and unauthorized use on information systems, and to check the effectiveness of information security measures, it is important to properly implement and use a monitoring function. When implementing the monitoring function, it is necessary to define the monitoring target and items in light of the characteristics of the information system and the classification of information handled on that information system.

Compliance Requirements

(1) Introduction and operation of the monitoring function

(a) Information system security officers shall formulate functional requirements for operation and management of the monitoring of information system operations and implement the monitoring function.

(b) Information system security officers shall properly operate the monitoring function implemented on the information system when operating the information system.

(c) Information system security officers shall periodically review the monitoring target and method for the information system in light of new threats and operating circumstances.

7.2 Measures against Information Security Threats

7.2.1 Measures against software vulnerabilities

Purpose

Potential threats against the information systems of Agencies include attacks such as third party intrusions to the systems resulting in the theft or destructions of important information belonging to the Agencies, as well as suspension thereof due to excessive workloads imposed by the third party. In particular, leakage of important information such as personal information could have an enormous impact on the daily lives of the general public and undermine public trust in the Agencies.

As for these types of threats, attackers commonly abuse vulnerability of software in the server, terminals, and communication line equipment which compose of information systems. Therefore, for information systems in Agencies, it is necessary to quickly and appropriately take measures against software vulnerabilities.

By the same token, the hardware of information systems may contain such vulnerabilities, so it is essential to refer to the provisions in section 5.2.2 “Information system procurement and configuration”, and to implement necessary measures.

Compliance Requirements

(1) Implementation of measures against software vulnerabilities

(a) When installing or starting operations of servers, terminals, and communication line equipment, information system security officers shall implement measures against publicly disclosed vulnerabilities of the software used on said equipment.

(b) When the publicly disclosed information about vulnerabilities is yet to be known, and applicable measures for servers, terminals, and communication line equipment are available, information system security officers shall implement such measures.

(c) Information system security officers shall regularly and as necessary verify the status of measures against vulnerabilities in the software used on servers, terminals, and communication line equipment.

(d) When it has been confirmed that measures against vulnerabilities have not been taken as a result of the regular verification of the status of such measures, or when information about vulnerabilities of the software used on servers, terminals, and communication line

equipment becomes available, information system security officers shall apply security patches, or establish plans for addressing software vulnerabilities and implement measures, after examining the effects upon information systems due to software updates and so on.

7.2.2 Measures for protection against malware

Purpose

If information systems were infected by malware, potential threats would be system breakdown and leakage of important information stored on said systems. Moreover, such infected information systems can spread infections to other systems, and possibly used as a platform to send spam e-mails and for denial-of-service attacks and so on, as well as a source of targeted attacks, which could give a threat to other entities and other information systems.

In order to prevent such incidents from occurring, it is necessary to duly implement measures against malware.

Compliance Requirements

(1) Implementations of measures against malware

(a) Information system security officers shall install anti-malware software and other tools on server equipment and terminals.

(b) Information system security officers shall take measures against malware, such as installing anti-malware software to protect all possible malware infection routes.

(c) Information system security officers shall regularly examine the implementation status of measures against malware as needed and take necessary measures.

7.2.3 Measures against denial-of-service attacks

Purpose

Potential threats against information systems accessed through the internet would be a denial-of-service attack by third parties, which disables legitimate users to access the services. Therefore, for the information systems of Agencies that are accessed through the internet, it is vital to take denial-of-service attacks into account and duly implement measures to ensure continuous availability of the systems. Recently, it is known that large-scale attacks by botnet consisting of so-called IoT (Internet of Things) devices connected to the Internet, or DDoS (Distributed Denial of Service) attack agency services that enable attacks without specialized technology or equipment exist. It is necessary to become more wary of those attacks.

Compliance Requirements

(1) Implementation of measures for denial-of-service attacks

(a) For information systems (referring to only those systems accessed through the internet, hereinafter the same in this section) handling vital information, system security officers shall implement measures for denial-of-service attacks, by using the functions incorporated in the equipment necessary for providing such services, like server equipment, terminals,

and communication line equipment, or the methods offered by private business providers, and so on.

(b) For information systems handling vital information, system security officers shall construct information systems equipped with tools which minimize impacts of denial-of-service attacks.

(c) For information systems handling vital information, system security officers shall identify equipment to be monitored among the server equipment, terminals, communication line equipment, and communication lines which are subject to denial-of-service attacks, and conduct monitoring.

7.2.4 Measures against targeted attacks

Purpose

Targeted attacks are attacks targeting a specific Agency, where attackers conduct a thorough investigation in advance, on the matters such as business practices and other internal information of the target, then make tenacious attacks with a combination of various types of attacks, applying the most effective method to violate the target Agency.

A typical and likely example of such attacks is the one made by unauthorized access or intruding into an information system of a certain Agency by some method, then expanding the intrusion areas by means of taking over access rights to steal or destroy critical information. As a series of such attacks may be made by using unknown methods, measures should be taken with the understanding that they can be difficult to perfectly detect and prevent.

It is necessary to be prepared for targeted attacks by establishing the multiple protection system for information security, which consists of measures to reduce targeted attack intrusions into information systems of the Agency (gateway measures), and measures for early detection and response to the intrusions, and measures to make expansion of intrusions harder (internal measures), as well as measures for detection and response to unauthorized communications with external entities (exit control measures).

Recently, not only direct attacks to organizations but also indirect attacks to organizations related thereto, such as subcontractors, are confirmed. It is required that a wider range of measures be considered.

Compliance Requirements

(1) Implementation of measures for targeted attacks

(a) Information security officers shall implement measures for information systems which reduce targeted attacks intrusions against the Agency (gateway measures).

(b) Information security officers shall implement measures for information systems to immediately detect and respond to the intruded attacks, and to make expansion of the intrusion harder, as well as to detect and respond to unauthorized communication with external entities (internal measures and exit control measures).

7.3 Zero Trust Architecture

7.3.1 Measures for implementing dynamic access control

Purpose

Conventionally, the "boundary model" measures (where certain trust in the internal network was delivered by placing a firewall as defense between external communication lines (e.g. Internet) and internal communication lines) were the most commonly used to protect information assets on the internal network of organizations. Due to the proliferation of cloud services and changes in the business system environment brought about by teleworking, the threats surrounding information assets in organizations are changing, making it more difficult to implement sufficient security measures for such new environments with only the defense available from the boundary model scheme. Notably, there is over-reliance on boundary measures to protect information assets such as server equipment placed within the boundary, which may indicate insufficient information security measures against cross-sectional infringement in the event of intrusion (also called lateral movement).
The zero trust architecture is a logical and structural concept for information security measures aimed at minimizing information security risks by protecting information assets based on the premise that networks are constantly intruded regardless of whether they are inside or outside of an organization. Furthermore, zero trust architecture is applied throughout the entire life cycle of medium-to-long-term government information systems and does not indicate a specific implementation or solution.
As one zero trust architecture-based measure to protect information assets, a mechanism can be built to continuously authenticate and approve the accessing entity, equipment accessing and being accessed, and status of software, service, network, etc. for each request to access information assets. This section describes measures particularly necessary for implementing the "dynamic access control," which is part of the function that realizes such mechanism.
When implementing a dynamic access control function, in addition to the requirements specified in this section, compliance with requirements for the introduction of user/entity authentication function specified in 7.1.1 "User/Entity authentication function," the introduction of access control function specified in 7.1.2 "Access control functions," and the authority control specified in 7.1.3 "Authority control" are also necessary. When implementing dynamic access control in an existing information system configuration, it is important to also review the software used for access control, as well as the configuration of the existing information system.

Compliance Requirements

(1) Assignment of person responsible for dynamic access control
   (a) When implementing dynamic access control among multiple information systems, the head information security officer shall assign an information system security officer as the person responsible for planning, promoting, and operating cross-system measures.

(2) Deliberation on the introduction policy for dynamic access control
   (a) When introducing dynamic access control, information system security officers shall identify the target information system resources for dynamic access control and establish

the introduction policy for dynamic access control.

(3) Measures for implementing dynamic access control
   (a) Upon implementing dynamic access control, information system security officers shall prepare an access control policy for dynamic access control (hereinafter referred to as "access control policy") according to the changes in the resource credit information.
   (b) Information system security officers shall implement dynamic access control based on the access control policy.

7.3.2 Measures for operating dynamic access control

Purpose

In light of the constantly changing form of resource usage due to the spread of teleworking and the Cloud-by-Default principle, when operating dynamic access control, it is important to check whether the measures reviewed during implementation are correctly functioning, and if necessary, review and revise the access control policy. If any risk is detected during the collection of resource credit information, which is the precondition of dynamic access control, it is necessary to take measures to reduce such risks.

This section only specifies the particularly necessary measures for Agencies to operate dynamic access control. Together with the requirements described in this section, it is also necessary to comply with the requirements for the management of identification codes and user/entity authentication information specified in 7.1.1 "User/Entity authentication function," the proper operation of access control specified in 7.1.2 "Access control functions," and the authority control specified in 7.1.3 "Authority control."

Compliance Requirements

(1) Review of the implementation policy for dynamic access control
   (a) Upon operating dynamic access control, information system security officers shall review the access control policy based on key changes in information security.

(2) Measures for operating dynamic access control based on resource credit information
   (a) Upon operating dynamic access control, information system security officers shall deal with risks detected during the collection of resource credit information.

Chapter 8 Use of Information Systems

8.1 Use of Information Systems

8.1.1 Use of information systems

Purpose

Employees use a wide range of information systems, including e-mail, web, and the systems for processing tasks on terminals, in order to execute their duties. There is a risk for information security incidents if these systems are not used appropriately.

Therefore, it is essential to maintain/establish provisions related to the use of information systems, and employees should comply with the provisions when using the systems.

Refer to Compliance Requirements in 6.1.2(1) for the establishment/maintenance of provisions related to Agency-furnished terminals (only when used outside of areas requiring control measures), and to Compliance Requirements in 6.1.3(2) for the establishment/maintenance of provisions related to non-Agency-furnished terminals.

Compliance Requirements

(1) Establishment/Maintenance of operating procedures related to the use of information systems

(a) The head information security officer shall establish/maintain operating procedures related to information security when using information systems at Agencies.

(b) The head information security officer shall establish operating procedures for handling information using external electromagnetic recording media, such as USB memory sticks.

(c) The head information security officer shall establish approval procedures for taking external electromagnetic recording media, such as USB memory sticks, to which confidentiality class-3 information, critical information, or vital information has been recorded outside of areas requiring control measures.

(2) Measures to encourage information systems users to comply with the provisions

(a) Information system security officers shall examine, from perspectives of information security risks and work efficiency, the scope of support functions which encourage employees to comply with the provisions, and shall construct the information systems equipped with such functions.

(3) Basic measures for the use of information systems

(a) Employees shall not use information systems for non-work related tasks.

(b) Employees shall not connect the information systems at their own Agencies to the communication lines other than the ones so authorized by information system security officers.

(c) Employees shall not connect the information systems which are not authorized by information system security officers, to the internal communication lines at Agencies.

(d) Employees shall not use any software that is not approved to use for the performance of

tasks. If using such software is required to execute tasks, an approval from the information system security officer shall be granted.

(e) Employees shall not connect unauthorized equipment, etc.to information systems,

(f) In such cases when an employee leaves the area where information systems are installed and there is a risk for unauthorized operation by third parties, he or she shall implement measures to protect the systems from unauthorized use.

(g) When taking external storage media, such as USB memory sticks, to which confidentiality class-3 information, critical information, or vital information has been recorded outside of areas requiring control measures, employees shall obtain the permission of the division/office information security officer.

(h) Employees shall not use any cloud service for which approval has not been given, even for use to perform tasks.

(4) Measures when using terminals (including non-Agency-furnished terminals)

(a) When handling classified information through the use of Agency-furnished terminals (only when used outside of areas requiring control measures) and non-Agency-furnished terminals, employees shall follow the prescribed usage protocols.

(b) When using the terminals listed in the following items to handle the information stipulated in the said items, employees shall obtain the permission of the division/office information security officer.

(i) Agency-furnished terminals (only when used outside of areas requiring control measures): Confidentiality class-3 information, critical information, or vital information

(ii) Non-Agency-furnished terminals: Classified information

(c) When connecting terminals (including non-Agency-furnished terminals) connected to communication lines outside the Agency outside of areas requiring control measures to communication lines inside the Agency in areas requiring control measures, employees shall take the established measures.

(5) Measures when using e-mail and web

(a) When sending and receiving e-mails containing confidential information, employees shall use e-mail services provided by the servers which are operated by, or outsourced by, their own Agencies.

(b) When sending and receiving information by e-mail to parties outside their own Agencies, employees shall use their government's domain name as the domain name of such e-mail's sender address, unless the government's domain name cannot be acquired.

(c) When receiving suspicious e-mails, employees shall handle them following the prescribed procedures.

(d) When it is necessary to review the web client settings, employees shall not make any setting changes which might impact on the information security.

(e) When downloading the software to the server equipment or terminals on which the web client is running, employees shall check the integrity of the software by verifying its distributor's digital signatures.

(f) When inputting and submitting the confidential information in a web form on the website they are viewing, employees shall ensure all of the followings.

(i) The contents to be submitted will be encrypted.

(ii) The website genuinely belongs to the organization where the contents are intended to.

(6) Handling of identification codes and user/entity authentication information

(a) Employees shall not use the information system by accessing the system through user/entity authentication with identification codes other than the ones assigned to them.

(b) Employees shall appropriately manage the identification codes assigned to them.

(c) If an employee is granted an identification code with administrator privileges, the use of such identification code shall be limited to only when they execute administrator's tasks.

(d) Employees shall manage their user/entity authentication information with utmost care.

(7) Measures for the use of encryption and digital signatures

(a) Employees shall follow the prescribed algorithms, key length, and methods when encrypting information, as well as assigning the digital signatures to the information.

(b) Employees shall follow the prescribed key management procedures, and appropriately manage the keys for decrypting the encrypted information, as well as those for assigning digital signatures to information.

(c) Employees shall take the backup of the key, following the prescribed backup procedures of the keys for decrypting the encrypted information.

(8) Prevention of malware infection

(a) Employees shall make efforts to implement measures against malware infection.

(b) If an employee becomes aware that an information system (including non-Agency-furnished terminals) could have been infected by malware, he or she shall implement necessary measures, such as to immediately disconnect the infected information system (including non-Agency-furnished terminals) from the communication lines.

(9) Measures when a web conference service is used

(a) Employees shall follow the specified procedures to implement information security measures according to participants in and information handled during a web conference.

(b) Employees shall, when holding a web conference, take measures so that any person not related to the conference is unable to participate therein.

(10) Measures for sharing information with a non-Agency entity by means of a cloud service

(a) When saving confidential information on a cloud service for the purpose of sharing information with a non-Agency entity, employees shall take measures to enable only those who need to share information to access the confidential information saved on the cloud service.

(b) When saving confidential information on a cloud service for the purpose of sharing information with a non-Agency entity, employees shall promptly delete the confidential information saved on the cloud service at the point when the information sharing becomes unnecessary.

8.1.2 Dissemination of information via social media

Purpose

Social media are now being generally used by Agencies for proactive public relations activities and other purposes. However, it is necessary to make sure that the citizens can verify whether the account is authentic, because the government domain name is inapplicable in such social media provided by the private sector. Furthermore, there is the possibility of hijacking of the Agencies' accounts, as well as a situation where vital information cannot be disseminated due to unannounced discontinuation of these social media. Therefore, when widely disseminating vital information to the citizens, it is necessary to consider methods of disseminating information to enable the citizens to access the original information sources. In addition, the originator of the information needs to implement measures against threats such as impersonation, to protect parties including the citizens from confusions caused by false information.

Also, these social media undergo rapid technology developments such as functionality expansion and additional services, so it is essential to promptly respond to changes in these external environments, including the business trends of the providers of such services.

Social media can be cloud services that become available only on consent to standard general terms and conditions, terms of services, etc., it is generally difficult to satisfy necessary and sufficient security requirements for the handling of confidential information. Therefore, social media shall be used only in cases where confidential information is not handled and the level of information management required for subcontractors is not high. When using social media, refer to the measures specified in 4.2.3 "Selection and use of cloud services to handle non-confidential information only."

Compliance Requirements

(1) Measures for dissemination of information via social media

(a) The head information security officer shall establish information security measures related to operational rules which include all of the following items, given that the social media are used with the accounts managed by Agencies. The head information security officer shall also stipulate that no confidential information should be handled when using such services.

(i) Measures to prevent impersonation, such as to clearly indicate the Agency which manages the accounts, in order to assure the information disseminated from accounts

of Agencies is genuinely originated from authentic Agencies

(ii) Measures to prevent unauthorized access, such as proper management of passwords and other information for user/entity authentication

(b) When using social media to provide vital information to the citizen, employees shall make such information available for viewing on their own Agencies' websites.

8.1.3 Teleworking

Purpose

While it is required that an environment in which flexible work styles are easily adopted be established and maintained pursuant to the execution plan for the realization of work style reform (Decision of the Council for the Realization of Work Style Reform on March 28, 2017), it is decided that employees are not always required to come to their working government offices for work for the performance of their own tasks, but are required to adopt a work style in which they perform their tasks remotely at home, a satellite office, or the like. Also in the situation where employees are requested to refrain from coming to their working government offices for work due to a large-scale disaster or as infection prevention measures for infectious disease, it is necessary to establish and maintain the teleworking environment so that most of employees are able to perform their tasks in any place other than their working government offices.

As Provision 8.1.3 only focuses on measures required for the implementation of teleworking only are provided. Therefore, in addition to this provision 8.1.3, refer to 3.1.1 "Information handling," 6.1.2 "Measures when using terminals outside areas requiring control measures," 6.1.3 "Measures for the adoption and use of non-Agency-furnished terminals," 6.4.1 "Communication lines," 6.4.2 "Communication line equipment," 6.4.3 "Wireless LAN," 7.1.6 "Monitoring function," and 8.1.1 "Use of information systems."

Compliance Requirements

(1) Establishment of operational rules

(a) The head information security officer shall establish operational rules related to information security measures when implementing teleworking. In principle, it shall be provided that teleworking shall be performed using Agency-furnished terminals.

(2) Measures for teleworking environment

(a) Information system security officers shall ensure information security for communication paths and against attacks peculiar to remote access when an information system that remotely accesses information systems at Agencies via communication lines outside the Agency due to the implementation of teleworking is constructed.

(b) Information system security officers shall perform multiple factor authentications for remote access.

(c) Information system security officers shall take measures so that terminals used for remote access are limited to approved terminals.

(d) Information system security officers shall limit terminals used for remote access to terminals on which the latest vulnerability or anti-malware measures are available.

(3) Measures for teleworking operations

(a) Information system security officers shall specify items to be checked by employees before and after the implementation of teleworking and have employees check such items.

(b) Employees shall select locations where teleworking is implemented so that shoulder surfing and eavesdropping can be prevented, and when implementing teleworking in any location other than at home, beware of theft while leaving their work desks.

(c) In principle, employees shall not implement teleworking using communication lines outside the Agency, on which information security measures are uncertain or insufficient.